

COPY

OCT 29 2024



CLERK OF THE SUPERIOR COURT
M. REYNA
DEPUTY CLERK

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

WILENCHIK & BARTNESS
A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW
The Wilenchik & Bartness Building
2810 North Third Street Phoenix, Arizona 85004

Telephone: 602-606-2810 Facsimile: 602-606-2811

Dennis I. Wilenchik, #005350
Tyler Q. Swensen, #015322
admin@wb-law.com
Attorneys for Plaintiffs

IN THE SUPERIOR COURT OF ARIZONA
IN AND FOR THE COUNTY OF MARICOPA

Maricopa County Republican Committee, a
political party county committee; Blaine "BJ"
Griffin, an individual and candidate seeking
election in 2024 to the Arizona House of
Representatives,

Plaintiffs,

v.

Maricopa County, Arizona; Maricopa
County Board of Supervisors; Jack Sellers,
Clint Hickman, Thomas Galvin, Bill Gates
and Steve Gallardo, in their capacity as
members of the Maricopa County Board of
Supervisors,

Defendants.

No. CV 2024-030770

**VERIFIED COMPLAINT
FOR SPECIAL ACTION**

(Redacted)¹

¹ Plaintiffs are filing this complaint and supporting exhibits in redacted form pursuant to
Ariz. R. Civ. P. 5.4(i)(1), and will be lodging an unredacted version with the Court along
with a Motion to File Under Seal pursuant to Ariz. R. Civ. P. 5.4(i)(2).

1 **INTRODUCTION**

2 1. Plaintiffs, Maricopa County Republican Committee (“MCRC”) and Blaine “BJ”
3 Griffin (“Griffin”), bring this Special Action to compel Maricopa County, Arizona (“County”),
4 the Maricopa County Board of Supervisors (“Board”), the individually named members of the
5 Board and any County election officials (collectively, the “Defendants”), to fulfill their official
6 duties including their duty to comply with Arizona election laws, in particular with regard to
7 ensuring the security of any passwords permitting access to the electronic voting systems
8 supplied by Dominion Voting Systems, Inc. (“Dominion”) that the County will utilize in the
9 2024 election on November 5, 2024.

10 2. Because Election Day is only six (6) days away, Plaintiffs have filed herewith an
11 Application for Order to Show Cause and ask the Court to set an expedited return date pursuant to
12 Rule 4, Arizona Rules of Procedure for Special Actions, as well as an expedited
13 hearing pursuant to Rule 57, Ariz. R. Civ. P.

14 3. Defendants have failed to acknowledge and have refused to address and rectify
15 serious violations of Arizona law and are thereby enabling and allowing potential unauthorized
16 access to the County’s voting systems that could result in manipulation of election results without
17 likely detection.

18 4. The Defendants’ employment of outside actors to conduct elections—a classic
19 insider threat vector—makes these violations even more acute. Indeed, earlier this summer, a
20 temporary election worker allegedly stole a security fob resulting in election equipment having to
21 be reprogrammed.²

22 5. As set forth in detail below, Arizona law expressly requires that: “[c]omponents of
23 the electronic voting system...[m]ust be password-protected (for voting system software)....
24 [and] passwords **must not be a vendor-supplied password and must only be known by**
25

26

² <https://www.cnn.com/2024/06/24/politics/arizona-election-worker-arrested-maricopa-county/index.html>

1 **authorized users.**” [2023 Election Procedure Manual (“EPM”) at p.102, (emphasis added),
2 relevant pages attached hereto as **Exhibit 1**; *See also* 2019 EPM at p.96 (same requirement),
3 relevant pages attached hereto as **Exhibit 2**].

4 6. Upon information and belief, Defendants have been violating and will continue to
5 violate both of these legal requirements by allowing vendor-supplied passwords to be used in its
6 election systems supplied by Dominion, thereby leaving open the potential for those machines to
7 be accessed by unauthorized users.

8 7. For example, one such vendor-supplied password [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED].³

12 8. In addition, passwords on the County’s election systems can be readily determined
13 by unauthorized users with a click of a few keystrokes.

14 9. The Defendants’ violations of the EPM’s password requirements pose a grave threat
15 to the security of the upcoming 2024 election. Anyone with licit or illicit access to the County’s
16 voting system can, among other things, unencrypt tabulator passwords on the County’s voting
17 system, as well as alter, fabricate, and transmit fraudulent election results, without likely detection.

18 10. Prior to initiating this lawsuit, on September 19, 2024, the MCRC put Defendants
19 on notice that the MCRC believed County was about to operate its electronic voting systems for
20 the upcoming 2024 election in a manner that violated the EPM’s requirements governing
21 passwords and other matters not at issue in this lawsuit. [*See* letter attached hereto as **Exhibit 3**].

22 11. The MCRC based its belief upon an examination of electronic data produced by the
23 County in connection with the 2020 and 2022 elections.
24
25

26 _____
3 [REDACTED]

1 12. The MCRC and the County engaged in several follow-up communications. [*See*
2 **Exhibit's 4 - 8** hereto].

3 13. Among other things, MCRC requested that the County confirm that any vendor-
4 supplied passwords would be removed from the County's election systems to be used in the 2024
5 election and that passwords would be protected from becoming known to unauthorized users.
6 [**Exhibit 3**, at p.3; **Exhibit 5**, at p.4].

7 14. Defendants have not only refused to agree to MCRC's requests, but with respect to
8 vendor-supplied passwords shown to exist on the County's election system, the County has stated
9 it "knows nothing about this and so can say nothing conclusively." [**Exhibit 6**, at p.5].

10 15. The County's admitted ignorance about its own election systems constitutes either
11 a willful violation of Arizona law, or, at a minimum, a cavalier and reckless disregard for the law's
12 requirements and whether they are being satisfied. Either way, the County's attitude does not
13 provide MCRC with any confidence that Defendants are following the law.

14 16. Indeed, instead of taking the situation seriously, the County threatened to seek
15 sanctions against undersigned counsel to intimidate them from filing this action.

16 17. Defendants each have duties to ensure elections are held with a "maximum degree
17 of correctness, impartiality, uniformity and efficiency on the procedures for early voting and
18 voting, and of producing, distributing, collecting, counting, tabulating and storing ballots." A.R.S.
19 § 16-452 (A).

20 18. Based on the responses provided by the County, Defendants appear to have either
21 abrogated their duties or fallen woefully short of fulfilling them and do not appear to be concerned
22 about them enough to ensure the County is adhering to the legal requirements as set forth
23 hereinabove.

24 19. MCRC therefore asks this Court to intervene and, as requested in the Application
25 for Order to Show Cause filed herewith, order Defendants to appear and show cause why the
26 Court should not hold them in contempt for failing and refusing to follow the law and fulfill their

1 duties under it to ensure that the County will be conducting the 2024 election in full compliance
2 with the aforesaid requirements of law.

3 20. The Arizona Constitution provides that “[a]ll elections shall be free and equal” and
4 no power ... shall at any time interfere to prevent the free exercise of the right [to vote].” Ariz.
5 Const. art. 2 § 21. To ensure this occurs, the Defendants should be ordered to be in full compliance
6 with the law as requested herein.

7 21. Special Action relief is appropriate here to compel government officials to perform
8 their governmental duties as required by law.

9 **PARTIES**

10 22. Plaintiff Maricopa County Republican Committee (“MCRC”) is a political party
11 operating as a non-profit entity under Arizona law in Maricopa County, and as such has a vested
12 interest in the elections in Maricopa County and the State of Arizona.

13 23. Plaintiff MCRC has standing to bring this action as an interested established
14 political party since its interests are directly affected by resolution of this matter regarding the
15 violations of Arizona law referenced above.

16 24. Plaintiff Blaine “BJ” Griffin is a candidate for LD22 Arizona House of
17 Representatives, an office he seeks in the 2024 Election.

18 25. Plaintiff Griffin is also a resident of the State of Arizona, registered to vote in
19 Maricopa County, who intends to vote in Arizona in the 2024 Election and has standing as an
20 intended voter in Maricopa County and candidate for Office to ensure the integrity of the election
21 process as well.

22 26. A justiciable controversy presently exists because the MCRC as a party putting forth
23 and supporting candidates for elected office and Griffin as a voter and a candidate for elected
24 office in Maricopa County, have the constitutional and statutory right to the accurate and
25 transparent tabulation of ballots such that only legal votes determine the winners of each contest
26 for public office.

1 27. Defendants' use of electronic voting systems with vendor supplied-passwords and
2 passwords that are known, or can be readily ascertained by unauthorized persons/entities
3 constitutes a grave potential threat to the integrity of the upcoming 2024 general election, that, at
4 a minimum, requires the Defendants to show cause why they should not be required to fully
5 comply with the law, and provide proof of that compliance, as requested by this action, which
6 Defendants to date have refused to supply

7 28. Defendants Jack Sellers, Clint Hickman, Thomas Galvin, Bill Gates and Steve
8 Gallardo, (collectively "Maricopa Individual Defendants") are being sued as members of the
9 Maricopa County Board of Supervisors ("Maricopa Board") for declaratory and injunctive relief
10 in their official capacities as members of the Maricopa Board.

11 29. The Maricopa Individual Defendants are all residents of Maricopa County, Arizona
12 and collectively have power over ensuring compliance with the law as set forth herein.

13 30. Under A.R.S. § 16-452 (A), the Maricopa Board is vested with the authority to:

- 14 • "[e]stablish, abolish and change election precincts, appoint inspectors and judges of
15 elections, canvass election returns, declare the result and issue certificates
16 thereof...";
- 17 • "[a]dopt provisions necessary to preserve the health of the county, and provide for
18 the expenses thereof";
- 19 • "[m]ake and enforce necessary rules and regulations for the government of its body,
20 the preservation of order and the transaction of business."

21 **JURISDICTION AND VENUE**

22 31. This Court has subject matter jurisdiction pursuant to Arizona Constitution Article
23 2, § 6.

24 32. This Court has personal jurisdiction over the members of the Board of Supervisors
25 as they all reside and conduct business in this County and State.

26 33. Venue is appropriate in this County pursuant to A.R.S. § 12-401.

1 34. This Court has authority to grant declaratory relief based on A.R.S. § 12-1831 et
2 seq., and to accelerate the hearing of this matter pursuant to Administrative Order of the Supreme
3 Court as an election matter, as well as under Rule 57, Arizona R. Civil Procedure.

4 35. This Court has jurisdiction to grant injunctive relief based on Arizona Rule of Civil
5 Procedure 65, as well as Rules 1-6, Rules of Procedure for Special Actions.

6 36. This Court has authority to award reasonable attorneys' fees and costs at its
7 discretion under A.R.S. § 12-349 and A.R.S. § 12-341.01 C.

8 FACTUAL ALLEGATIONS

9 **A. Background**

10 37. Arizona law expressly requires that: “[components of the electronic voting
11 system....[m]ust be password-protected (for voting system software).... [and that] passwords
12 must not be a vendor-supplied password and must only be known by authorized users.” [**Exhibit**
13 **1; Exhibit 2**].

14 38. The election procedures detailed in the EPM have the force and effect of law, and
15 violations of those procedures may also be subject a violator to criminal penalties. A.R.S. §16-
16 452(C); *See also Ariz. Pub. Integrity All. v. Fontes*, 250 Ariz. 58, 63 (2020).

17 39. In any electronic voter system, there are multiple levels of password protected
18 control privileges—from basic access to the system such as a Windows log-in to control over
19 election data/results and the election software itself.

20 40. Arizona law governing passwords is designed to give Arizonans assurance that the
21 outcome of elections in which they participate represents the true will of the People by preventing
22 unauthorized access or control over electronic voting machines and election results.

23 41. The County has contracted with Dominion Voting Systems to provide machines,
24 software, and services for the 2020 and 2022 elections and intends to rely on Dominion's
25 electronic voting systems to record and tabulate *all* votes cast in the 2024 general election held in
26 this county.

1 42. Dominion, manufactures, distributes, and maintains voting hardware and software.
2 Dominion also executes software updates, fixes, and patches for its voting machines and election
3 management systems. By its own account, Dominion provides an “End-To-End Election
4 Management System” (the “EMS”) that “[d]rives the entire election project through a single
5 comprehensive database.” Dominion’s tools “build the election project,” and its technology
6 provides “solutions” for “voting & tabulation,” and “tallying & reporting,” and “auditing the
7 election.” The products sold by Dominion include ballot marking machines, tabulation machines,
8 and central tabulation machines, among others.

9 43. The County has chosen to operate a “vote center model” pursuant to the EPM and
10 in the two most recent general elections had more than 200 vote centers, each with two Dominion
11 tabulators, along with Dominion tabulators and the Dominion Election Management System
12 server (“EMS”) at its central count location, the Maricopa County Tabulation and Election Center
13 (“MCTEC”).

14 44. The Defendants have turned over significant aspects of conducting the County’s
15 elections to Dominion including hiring Dominion employees like Bruce Hoenicke who have been
16 given administrative and technician privileges to Maricopa’s elections system including control
17 over the programming of election function. Maricopa officials also stated in 2021 that they do not
18 possess credentials necessary to validate tabulator configurations and independently validate the
19 voting system prior to an election. Dominion purportedly maintains those credentials.

20 **B. The County’s voting machines are configured with vendor-supplied**
21 **passwords in violation of Arizona law.**

22 45. An inspection of the County’s 2020 election database revealed that Dominion
23 inserted multiple common usernames and passwords [REDACTED]

24 [REDACTED].

25 46. Two examples of unlawful vendor-supplied passwords discovered on the County’s
26 election systems are [REDACTED]

1 47. Incredibly, the first password [REDACTED]

2 [REDACTED]
3 [REDACTED]⁴ [Declaration of Clay Parikh, at ¶¶ 12, 24-26, attached hereto as **Exhibit 9**].

4 48. With these passwords, Dominion or any other actor with licit or illicit access to
5 Maricopa County’s voting system can manipulate the voting system and alter election data and
6 election results. [*Id.*].

7 49. Notably, the County stated that with respect to the MCRC pointing out to it that as
8 to the “Dominion inserted ‘common’ usernames and passwords into [the County’s] voting systems,
9 [t]he County *knows nothing about this and so can say nothing conclusively.*” [Exhibit 6, at p.5
10 (emphasis added)].

11 50. The County’s lack of awareness or concern about their own voting systems and an
12 apparent wholesale delegation of their election duties to Dominion is a disturbing breach of
13 election security that Arizona laws are intended to prevent.

14 51. And this is not the first time that the County claimed ignorance about Dominion’s
15 activities in running the County’s elections with respect to password credentials. In connection
16 with the Arizona Senate audit of the 2020 election, the County stated it could “not produce any
17 credentials to access the higher level administrative or configuration settings for the tabulators....
18 [claiming that] only the contracted Dominion employees have access to these credentials.” As a
19 consequence of turning over password access of its election systems to Dominion, the County
20 does not have any way to independently validate its own voting system.

21 52. In addition, [REDACTED]

22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]. [Exhibit 9, ¶¶ 24-26].
26 _____

⁴ [REDACTED]

1 53. Given the County’s claimed ignorance of vendor-supplied passwords on its election
2 systems, it is likely these [REDACTED] passwords still exist on the County’s
3 election systems. And an untold number of individuals obviously may know these passwords. The
4 potential risks and consequences of this security violation are grave.

5 **C. Passwords in the County’s voting machines can be readily revealed by**
6 **unauthorized users rendering those passwords discoverable to unauthorized**
7 **users in violation of Arizona law.**

8 54. In addition, the vendor-supplied passwords in the table Figure A-3 to the Parikh
9 Declaration can be used to control the election software and election data/results, can be
10 discovered by unauthorized parties with a few simple keystrokes rendering any protection
11 afforded by them meaningless—as well as violating Arizona law requiring passwords to only be
12 known by an authorized user.

13 55. Specifically, while these passwords are stored in both hash form and encrypted
14 within the election database, they are unprotected. [Exhibit 9, ¶ 26].

15 56. Thus, anyone who can gain access to the database can copy the hash or encrypted
16 password and can discover the plain text password through widely available websites. [*Id.*].

17 57. For example, one common hash for several County administrative accounts can
18 easily be cracked—and thus be discovered by unauthorized users using a public web site
19 “hashes.com”. [*Id.*]. Thus, these passwords can readily become known by unauthorized users in
20 violation of Arizona law.

21 **D. The x509 certificate vendor-supplied authentication code acts as a password**
22 [REDACTED]

23 58. Lastly, the x509 certificate used by the County voting system [REDACTED]
24 [REDACTED] is therefore clearly vendor-
25 supplied, and [REDACTED]
26 [Exhibit 9, ¶ 15].

1 59. The security certificate serves the same function of authentication as a password by
2 allowing a system or a system component to authenticate and/or trust and thereby access another
3 system or system component to transfer election data and results. [*Id.*].

4 60. This common certificate, [REDACTED]
5 [REDACTED] is known to an untold number of individuals outside of the County, in violation of Arizona
6 law, and creates an unacceptable potential for an unauthorized user to gain access to the County's
7 election system and manipulate election results. [**Exhibit 9**, ¶¶ 11, 15, 20, 30].

8 **E. There is a substantial risk of imminent and grave injury**

9 61. All persons who vote in the 2024 General Election, if required to vote using an
10 electronic voting system or have their vote counted using an electronic voting system, will be
11 irreparably harmed unless the County complies with the law.

12 62. Because the County is using vendor-supplied passwords and/or passwords that are
13 known or can be readily become known to unauthorized users in violation of express Arizona law
14 there is a continuing risk of irreparable harm that may not be able to be repaired and is not
15 remediable by damages.

16 63. With these passwords, a person with licit or illicit access to the County's election
17 system can manipulate the voting system and alter election data and election results. The
18 consequences of such manipulation and their impact on the democratic process are terrifying to
19 contemplate.

20 64. Because of what appears to be a clear violation of Arizona law, the County's voting
21 system does not reliably ensure trustworthy and verifiable election results, and the County has not
22 been able to provide conclusive evidence that it is in full compliance with the law's requirements.

23 65. There is no other equally plain, speedy, or reliable remedy available for this situation
24 and monetary damages will not suffice as the injury is unique.

25 66. Each of the foregoing harms to Plaintiffs are imminent for standing purposes
26 because the 2024 General Election is set to occur.

1 **CLAIMS**

2 **COUNT I: VIOLATION OF ARIZONA LAW**

3 *(Seeking special action, declaratory and injunctive relief against all Defendants)*

4 67. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

5 68. The right to vote is a fundamental right protected by Article 2, Sections 4 and 21 of
6 the Arizona Constitution.

7 69. The fundamental right to vote encompasses the right to have that vote counted
8 accurately, and it is protected by Article 2, Section 4 of the Arizona Constitution.

9 70. Defendants have violated Plaintiffs' fundamental right to vote by allowing vendor
10 supplied passwords on the County's election systems, [REDACTED]
11 and passwords that can be easily revealed to unauthorized users presenting a clear and present
12 danger to the right of Plaintiff's and others to have confidence in the voting system employed by
13 the Defendants. Defendants have been put on notice to perform their governmental function to
14 correct the violation of law and have ignored the demands for adequate assurances of compliance.

15 71. Defendants' willful violations of law will continue in the 2024 Election and beyond
16 if not stopped.

17 72. Plaintiffs ask this Court to declare that these Defendants violated Article 2, Section
18 4 of the Arizona Constitution; remedy the County's electronic voting systems to comply with
19 Arizona law governing passwords for elections systems as detailed herein for the 2024 Election
20 and beyond; and to compel them as governmental officials to simply comply with the law and
21 award attorneys' fees and costs to Plaintiffs for Defendants' failure to comply, causing this lawsuit
22 to be filed.

23 73. Unless Defendants are enjoined by this Court to not continue the practice, or
24 compelled by the Court to perform their function in overseeing the election process in the County
25 according to law, then Plaintiffs will have no adequate legal, administrative, or other remedy by
26 which to prevent or minimize the irreparable, imminent injury that is threatened by Defendants'

1 conduct. Accordingly, injunctive and/or special action relief against these Defendants is warranted
2 to require they conduct this election per the legal requirements of this State and the laws
3 promulgated thereunder.

4 **COUNT II: VIOLATION OF A.R.S. § 11-251**

5 74. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

6 75. Defendants, as members of the County Board, are charged with statutory duties to
7 electors in Arizona, including Plaintiffs, under A.R.S. § 11-251.

8 76. Defendants have failed to meet the duties set forth in A.R.S. § 11-251 to adopt
9 provisions necessary to preserve the elections in the County.

10 77. Defendants have failed to meet the duties set forth in A.R.S. § 11-251 to make and
11 enforce necessary rules and regulations for the government of the County to preserve order and to
12 transact business, to wit: election laws designed to protect the election process as complained of
13 herein.

14 78. Defendants intend to continue in their failure to meet these duties through the 2024
15 Election if this Court does not order them to comply with the laws.

16 79. Plaintiffs have a private right of action against Defendants under Arizona law.

17 80. Unless Defendants are enjoined by this Court, or special action relief is granted to
18 compel them to perform their governmental function at law, then Plaintiffs will have no adequate
19 administrative, or other remedy by which to prevent or minimize the irreparable, imminent injury
20 that is threatened by the intended conduct of Defendants. Accordingly, injunctive and/or special
21 action relief against Defendants is warranted.

22 **COUNT III: DECLARATORY JUDGMENT – A.R.S. § 12-1831, et seq.**

23 81. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

24 82. Defendants' conduct will have the effect of violating the rights of the citizens of
25 Arizona, as described above.

1 83. The Court has the authority pursuant to A.R.S. § 12-1831, et seq. to issue an Order
2 to Show Cause and an Order declaring the respective rights and obligations of the parties with
3 respect to enforcing the law as set forth herein relating to the protection of passwords to the voting
4 systems to be used in Maricopa County elections. This is a justiciable controversy that is ripe for
5 such determination as Defendants have failed and or refused to assure Plaintiffs that they are in
6 compliance with the letter of the law as set forth herein.

7 84. If the County is allowed to proceed with an election as described above, it will
8 violate the rights of the citizens of the State by conducting an election with an unsecure, vulnerable
9 electronic voting system which is susceptible to manipulation and intrusion.

10 85. Because of the issues described above regarding the election system and processes
11 to be used by Defendants which is believed to be in violation of the law, the Court should issue
12 an Order declaring that it is a violation of the laws of this State, for the County to conduct an
13 election which relies on the use of electronic voting systems to cast or tabulate the votes that are
14 not reliable or vetted per the statutory requirements as set forth herein.

15 **PRAYER FOR RELIEF**

16 WHEREFORE, Plaintiffs respectfully request that this Court:

17 1. Enter a preliminary and permanent injunction prohibiting Defendants from
18 requiring or permitting voters to cast votes using tabulated electronic voting systems that do not
19 comply with the laws of this State, and requiring:

- 20 a) the County's election systems no longer employ *any* vendor-supplied
21 passwords, including any vendor-supplied encryption keys, as mandated by
22 the EPM.
- 23 b) the County's current passwords be protected and restricted such that they are
24 known only to authorized users as mandated by the EPM and cannot be
25 revealed to or discovered by an unauthorized user.

26 a) Enter an Order declaring the law of the State that Defendants must follow and

1 directing Defendants to conduct the 2024 Election consistent with that law.

2 2. In the alternative, in the event the Court is unwilling to grant the preliminary and
3 permanent injunction sought above, to ensure transparency in the 2024 Election and remedy the
4 uncertainty caused by Defendants' violations of Arizona law, order Defendants to produce or
5 make the following records available to the MCRC for copying, downloading and/or inspection
6 beginning within 24 hours of the close of the polls on November 5, 2024, with productions
7 continuing every 24 hours for any additional records identified below until the election has been
8 certified:

9 a) All vote center and central count tabulator system logs beginning with the
10 first use of any voting system component for the 2024 general election (e.g., ballot design,
11 election event design, or any testing (including any L&A testing));

12 b) All vote center tabulator open and close poll tapes beginning with the first
13 use of any voting system component for the 2024 general election as described above.

14 c) All vote center and central count Cast Vote Record reports in an unaltered
15 state (e.g., including all data fields and in batch order i.e., not randomized except within batch).

16 d) The written reports mandated by A.R.S. § 16-442 "comparing the number
17 of votes cast as indicated on the machine or tabulator with the number of votes cast as indicated
18 on the poll list and the number of provisional ballots cast" for each vote center.

19 3. Order an accelerated hearing on the declaratory relief sought per Rule 57, Arizona
20 R. Civil Procedure.

21 4. Order that the Court shall retain jurisdiction to ensure Defendants' ongoing
22 compliance with the foregoing Orders, and appoint a Special Master to ensure compliance with
23 the law.

24 5. Grant Plaintiffs an award of their reasonable attorney's fees, costs, and expenses
25 incurred in this action pursuant to A.R.S. § 12-349 or 12-341.01 (C) or under the private Attorney
26 General doctrine.

1 6. Granting such other and further relief as to the Court appears just and proper.

2 **FILED on October 29, 2024.**

3 **WILENCHIK & BARTNESS, P.C.**

4 */s/ Dennis I. Wilenchik*
5 Dennis I. Wilenchik, Esq.
6 Tyler Q. Swensen, Esq.
7 The Wilenchik & Bartness Building
8 2810 North Third Street
9 Phoenix, Arizona 85004
10 admin@wb-law.com
11 *Attorneys for Plaintiffs*

12 RETRIEVED FROM DEMOCRACYDOCKET.COM

13
14
15
16
17
18
19
20
21
22
23
24
25
26

VERIFICATIONS

Craig Berland, upon his oath, states as follows:

1. I am the Chairman of the Maricopa County Republican Committee, a named Plaintiff in this action and in that capacity, I am authorized to sign this Verification on behalf of MCRC.

2. I make this Verification based on my own knowledge, as well as information and belief.

3. I have reviewed the Verified Special Action Complaint and attest under penalty of perjury that the allegations therein are true and accurate to the best of my knowledge, information, and belief.

DATED: 10/29/2024

DocuSigned by:
Craig Berland
66ADF0A4EB6E4DE...
Craig Berland

Blaine Griffin, upon his oath, states as follows:

1. I am a named Plaintiff in this action and make this Verification based on my own knowledge, as well as information and belief.

2. I have reviewed the Verified Special Action Complaint and attest under penalty of perjury that the allegations therein are true and accurate to the best of my knowledge, information, and belief.

DATED: 10/29/2024

Signed by:
Blaine C. Griffin Sr
585EEFCC42ED4B0...
Blaine Griffin

EXHIBIT 1

RETRIEVED FROM DEMOCRACYDOCKET.COM

WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —



State of Arizona

2023

**ELECTIONS
PROCEDURES
MANUAL**



ADRIAN FONTES
SECRETARY OF STATE
STATE OF ARIZONA

Arizona Department of State - Office of the Secretary of State
1700 W. Washington St., FL 7, Phoenix, Arizona 85007

azsos.gov | 1-877-THE VOTE (843-8683)

B. Data Security of the Electronic Voting System

Components of the electronic voting system:

1. Must be password-protected (for voting system software);⁴⁵
 - In addition to complying with any system requirements, passwords must not be a vendor-supplied password and must only be known by authorized users.
2. May not be connected to the internet, any wireless communications device, or any external network (except for e-pollbooks);
 - An EMS must be a stand-alone system, attached only to components inside an isolated network. An EMS may only be installed on a computer that contains only an operating system, the EMS software, data/audio extractor software, and any necessary security software.
3. May not be used to modem election results, whether through analog, cellular, or any similar transmission;
4. May not contain remote access software or any capability to remotely access the system;
5. Must match the software or firmware hash code on file with the officer in charge of elections prior to programming the election and the hash code on file with either (1) the National Institute of Standards and Technology (NIST); or (2) the Secretary of State at the time of certification of the electronic voting system; and
 - If the EMS software hash code is on file with NIST or the Secretary of State, the officer in charge of elections must certify that the officer compared the hash code on file with NIST or Secretary of State for the EMS software with the hash code of the EMS software to be used in the election and certify that the numbers are identical.
6. Must be observed by the officer in charge of elections or a designee if the election program (or any software or firmware) is updated or modified.

In addition, the County Recorder or officer in charge of elections should retain back-ups of the election program, including daily back-ups once tabulation begins.

C. Removable Electronic Storage Devices Used with the Voting System

The following security protocols apply to any memory stick or other removable electronic storage device used with the electronic voting system:

1. A stick or device must be purchased or received from a reliable source.
2. A stick or device shall be permanently identified with a unique serial number or identifier when in use, and an inventory of all electronic media shall be created and maintained.

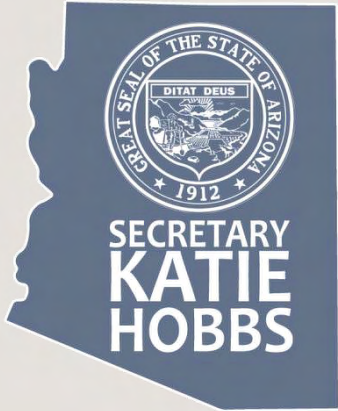
⁴⁵ Counties and their IT staff should also consult the latest standards for password security from the National Institute of Standards and Technology (NIST), available at <https://pages.nist.gov/800-63-3/sp800-63-3.html>.

EXHIBIT 2

RETRIEVED FROM DEMOCRACYDOCKET.COM

WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —

WB



STATE OF ARIZONA

2019 ELECTIONS PROCEDURES MANUAL

December 2019

www.azsos.gov



1700 W. Washington St. Phoenix, AZ 85007



1-877-THE-VOTE (843-8683)



RETRIEVED FROM DEMOCRACYDOCKET.COM

written log or with electronic key card access that indicates the date, time, and identity of the person accessing the system.

4. Must be sealed with tamper-resistant or tamper-evident seals once programmed;
 - The seal number must be logged as corresponding with particular voting equipment and the election media that has been sealed in the voting equipment. The log should be preserved with the returns of the election. In the event of a recount or re-tally of votes, the officer in charge of elections should be prepared to submit an affidavit confirming that the election program and any election media used in the election have not been altered. [A.R.S. § 16-445\(C\)](#).
5. Must be safeguarded from unauthorized access when being moved, transferred, serviced, programmed, or temporarily stored;
6. May be accessed by elections staff only to the extent necessary to perform their authorized task; and
7. Must be witnessed by two or more election staff members (of different political parties if possible) when being moved or transferred, which includes an inventory of the equipment and chain of custody before and after the move or transfer.

B. Data Security of the Electronic Voting System

Components of the electronic voting system:

1. Must be password-protected (for voting system software);
 - In addition to complying with any system requirements, passwords must: (1) contain mixed-cased and non-alphabetic characters, if possible; (2) be changed on a regular basis and may not be a vendor-supplied password; and (3) may be known only by authorized users.
2. May not be connected to the internet, any wireless communications device, or any external network (except for e-pollbooks);
 - An EMS must be a stand-alone system, attached only to components inside an isolated network. An EMS may only be installed on a computer that contains only an operating system, the EMS software, data/audio extractor software, and any necessary security software.
3. May not be used to modem election results, whether through analog, cellular, or any similar transmission;
4. May not contain remote access software or any capability to remotely-access the system;
5. Must match the software or firmware hash code on file with the officer in charge of elections prior to programing the election and the hash code on file with either (1) the National Institute of Standards and Technology (NIST); or (2) the Secretary of State at the time of certification of the electronic voting system; and
 - If the EMS software hash code is on file with NIST or the Secretary of State, the officer in charge of elections must certify that the officer compared the hash code on file with

EXHIBIT 3

Redacted

RETRIEVED FROM DEMOCRACYDOCKET.COM

WILENCHIK & BARTNESS

— A PROFESSIONAL CORPORATION —

OLSEN LAW, P.C.

KURT B. OLSEN

ATTORNEY AT LAW

1250 CONNECTICUT AVENUE, N.W., SUITE 700, WASHINGTON, DC 20036

(202) 408-7025

KO@OLSENLAWPC.COM

September 19, 2024

Via Email

Rachel Mitchell
Maricopa County Attorney
225 West Madison Street
Phoenix, AZ 85003

**Re: Pre-Litigation Demand Letter Regarding Maricopa County's
Non-Compliance With Arizona Election Law**

Dear Counsel:

On behalf of the Maricopa County Republican Committee (the "Client" or "MCRC"), this letter is a pre-suit litigation demand that Maricopa County ("Maricopa") take action to provide a secure and accurate election in the upcoming 2024 general election in light of three clear past and potentially continuing violations of Arizona election law. As you know, a forensic inspection of tabulator log files and other voting system data produced by Maricopa showed that:

- (1) Maricopa employed vendor-supplied encryption keys placed unprotected and in plain text on Maricopa's election system in violation of EAC-certification requirements.¹ With these keys, Dominion—and anyone with licit or illicit access to Maricopa's voting system—can, among other things, alter or fabricate election results and unencrypt tabulator passwords on Maricopa's voting system. In addition, it appears that the vendor, Dominion Voting Systems ("DVS"), inserted multiple common usernames and passwords [REDACTED]. These passwords and username combinations were present in DVS computing devices that were used in previous elections. Two combined vendor supplied credentials allow Dominion, or anyone else with knowledge of the credentials, to bypass the Windows-login, access the SQL election database and/or the EMS—thereby providing

¹ The encryption keys are: the Rijndael Key; the Rijndael Vector; the X509 Certificate; and the Hash-Based Message Authentication Code ("HMAC"). Dominion's operative and past contracts with Maricopa, Serial 190265-RFP, state that: "Data generated by the Democracy Suite platform, including results reporting, is *protected* by the deployment of FIPS-approved symmetric AES and asymmetric RSA encryption." This indicates that Dominion supplies these encryption keys, which meet the definition of a password given their function.

unfettered access to the SQL server function and databases and allowing total control over the election data and results (as well as the encryption keys).²

Arizona law requires that all voting system passwords “*not be a vendor-supplied password and must only be known by authorized users.*” 2023 Election Procedure Manual (“EPM”) at p. 102. *See also* 2019 EPM at 96 (same requirement). The circumstances described above plainly violate these requirements.

- (2) Maricopa employed altered election software not approved for use in Arizona in accordance with A.R.S. § 16-442, and falsely represented that it used Dominion Voting Systems (“DVS”) Democracy Suite 5.5B election software certified by the Election Assistance Commission, including that the hash values matched with the certified software.³
- (3) In connection with the 2020 and 2022 general elections, Maricopa certified it successfully conducted statutorily mandated pre-election logic and accuracy (“L&A”) testing on October 6, 2020 and October 11, 2022, respectively. In fact, Maricopa tested only five spare tabulators on those dates. After the 2022 election, an inspection of the tabulator log files revealed Maricopa’s 400+ vote center tabulators had initialization dates of October 14, 17-18, 2022 *i.e.*, after the October 11, 2022 L&A test. Maricopa then admitted under oath that it had installed reformatted memory cards with election software on all 400+ vote center tabulators *after* the October 11, 2022 L&A test. Maricopa also admitted that it did not perform L&A testing on those tabulators after that election software installation in accordance with A.R.S. § 16-449.

As you know, Maricopa claimed under oath that this installation of reformatted memory cards with election software (post-L&A test) was purportedly due to Maricopa’s discovery of a mistake in the election software programming on October 10, 2022, which supposedly was corrected prior to the October 11, 2022 L&A test. However, the tabulator logs files from the 2020 general election show Maricopa apparently did the same thing in that election *i.e.*, the vote center tabulators have initialization dates that begin October 7, 2020—*i.e.*, *after* the October 6, 2020 L&A

² The redacted passwords are [REDACTED]. The full passwords are available upon request, but you should be capable of checking your systems, including the EMS, tabulators, and adjudication computers, for *any other* vendor supplied passwords including any vendor supplied passwords that *may have been* included in the recent upgrade to DVS Democracy Suite version 5.17.

³ As noted in note 2, we are aware that Maricopa apparently recently upgraded its election software to DVS Democracy Suite version 5.17.

test.⁴ This indicates Maricopa has a practice of installing reformatted memory cards with election software *after* the official L&A test date without performing L&A testing on those tabulators in accordance with A.R.S. § 16-449.

In light of the aforementioned repeated and deliberate violations of law, on behalf of the MCRC, we ask that Maricopa confirm the following in writing by Thursday, September 26, 2024:

1. Maricopa's election systems no longer employ *any* vendor-supplied passwords, including any vendor-supplied encryption keys, as mandated by the EPM.
2. Maricopa's current passwords can only be known by authorized users, as mandated by the EPM, and cannot be decrypted by any encryption key known by DVS or decrypted or derived by any unauthorized user.
3. DVS Democracy Suite version 5.17, as approved by the Arizona Secretary of State in accordance with A.R.S. § 16-442, has been installed on all Maricopa election systems and components (including the EMS, all ICP2 and ICC tabulators, and all components used, including ballot marking devices).
4. The election software Maricopa used in the 2020 and 2022 elections, and any software not approved by the Arizona Secretary of State does not now reside on any of these components identified above, nor on any removable media in Maricopa's possession or accessible to any person or office with physical access to Maricopa voting systems.
5. After the completion of the official statutorily announced and compliant L&A test scheduled to take place on or about October 7, 2024, Maricopa will *not* reformat or alter the L&A tested software configuration on any memory cards of any tabulator, or install any election software on any tabulator, without conducting a statutorily compliant L&A test on those tabulators in accordance with A.R.S. § 16-449 after taking such actions.
6. That Maricopa will produce or make the following records available to the MCRC for copying, downloading and/or inspection beginning within 24 hours of the close of the

⁴ You were previously put on notice of these violations of law and supporting evidence by the petition for writ of certiorari filed in *Lake et al. v. Fontes*, No. 23-1021 (U.S.) on March 18, 2024 (the "*Lake/Finchem* Action"), as well as by my April 2, 2024 letter to you regarding your violations ARIZ. R. PROF'L. COND. 3.3(a)-(c) related to the *Lake/Finchem* Action, and by the motion to recall the mandate filed with the Ninth Circuit related to that same action.

September 19, 2024

Page 4

polls, with productions continuing every 24 hours for any additional records identified below until the election has been certified:

- a. All vote center and central count tabulator system logs beginning with the first use of any voting system component for the 2024 general election (*e.g.*, ballot design, election event design, or any testing (including any L&A testing)).
- b. All vote center tabulator open and close poll tapes beginning with the first use of any voting system component for the 2024 general election as described above.
- c. All vote center and central count Cast Vote Record reports in an unaltered state (*e.g.*, including all data fields and in batch order *i.e.*, not randomized beyond the batches of one hundred ballots).
- d. The written reports mandated by A.R.S. § 16-442 “comparing the number of votes cast as indicated on the machine or tabulator with the number of votes cast as indicated on the poll list and the number of provisional ballots cast” for each vote center.

If we do not receive a response from Maricopa by the close of business, Thursday, September 26, 2024, the MCRC has authorized litigation to compel the County to do so and to prevent Maricopa from repeating its prior violations of Arizona election law.

Sincerely,

A handwritten signature in black ink, appearing to read 'K.B. Olsen', with a long horizontal line extending to the right.

Kurt B. Olsen

Cc: Dennis I. Wilenchik
Thomas P. Liddy

EXHIBIT 4

RETRIEVED FROM DEMOCRACYDOCKET.COM

WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —

WB



Maricopa County Attorney

RACHEL MITCHELL

September 26, 2024

VIA EMAIL ONLY

Kurt Olsen
1250 Connecticut Avenue, N.W.
Suite 700
Washington, DC 20036

RE: Your September 19, 2024, “pre-litigation demand letter”

Mr. Olsen,

I received the letter you sent to the County Attorney, dated September 19, 2024, and claiming to be a “pre-litigation demand letter” (the “Letter”). Maricopa County complies with all federal and state laws that govern elections, and the Letter’s assertions to the contrary are false. These and other allegations have been presented to various courts of competent jurisdiction over the past several years by yourself and others and have failed. Courts have repeatedly found that Maricopa County’s elected officers and elections administration professionals follow the law and have also repeatedly confirmed the results of elections conducted in Maricopa County.

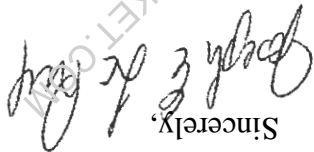
Contrary to your false allegations, all tabulators used in the 2020, 2022, and 2024 elections underwent pre-election logic and accuracy testing, including the spares that were not ultimately deployed. Further, all tabulators that will be used in the 2024 general election (including the spares held in reserve) will undergo pre-election logic and accuracy testing.

Also contrary to your false allegations, the Dominion Democracy Suite version installed on the County’s election equipment was certified by both the federal Election Assistance Commission and the Secretary of State.

Discussing our clients’ election-related security operations with you could compromise the ability of our clients to ensure the security of its election administration. We will not do that. We will only say that your allegations in the Letter about the security of the County’s election systems reveal a substantial misunderstanding on your part of the law’s requirements and the County’s actual practices and procedures.

Marricopa County declines your invitation to substitute your client's election procedure preferences for those codified in Arizona law by the Legislature and the Governor, plus the directives placed in the Elections Procedures Manual by the Secretary of State, the Attorney General, and the Governor. Should your client wish to have their preferred procedures followed in Arizona in future elections, they should lobby the state legislature.

Finally, we are not aware that you are a member of the Arizona Bar or that you are admitted *pro hac vice* for this matter. Please let us know if there is an Arizona attorney with whom we should be discussing this matter in the future.

Sincerely,


Joseph E. La Rue
Deputy County Attorney
Marricopa County Attorney's Office

Cc: Dennis Wilenchik

RETRIEVED FROM DEMOCRACY
ARCHIVE.ORG

EXHIBIT 5

Redacted

RETRIEVED FROM DEMOCRACYDOCKET.COM

WILENCHIK & BARTNESS

— A PROFESSIONAL CORPORATION —



Dennis I. Wilenchik
diw@wb-law.com

WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —
ATTORNEYS AT LAW
The Wilenchik & Bartness Building
2810 North Third Street Phoenix Arizona 85004

Licensed in
Arizona, Texas
and New York

Telephone: 602-606-2810 Facsimile: 602-606-2811

September 28, 2024

Via Email and Regular Mail

Joseph E. La Rue, Esq.
Deputy County Attorney
Maricopa County Attorney's Office
225 West Madison Street
Phoenix, AZ 85003

Re: Maricopa County's response to MCRC's Pre-Litigation Demand Letter Regarding Maricopa County's Non-Compliance With Arizona Election Law

Dear Joe:

First, best personal regards. Thank you for your response to the MCRC's pre-litigation demand letter. However, after review I have to say it repeats Maricopa's failure to address conclusive forensic evidence, and therefore is disturbing to me. It is my understanding that there is evidence that recently confirms Maricopa repeatedly violated Arizona law in connection with the 2020 and 2022 elections. Contrary to your assertions, neither Maricopa nor any court has substantively addressed these facts and the evidence directly, much less ruled on, the forensic evidence conclusively demonstrating Maricopa's violations of election law. Maricopa's refusal to address this, and the evidence, makes it clear that it has no real response other than to rely on decisions where that evidence was never really examined. Thus, MCRC's concerns that Maricopa will repeat its violations of Arizona law in the upcoming 2024 election are all the more acute. And, from my perspective, we could resolve those issues in good faith with your cooperation.

First, as was pointed out in our pre-litigation demand letter, Arizona law expressly requires that all voting system passwords “*not be a vendor-supplied password and must only be known by authorized users.*” 2023 Election Procedure Manual (“EPM”) at p. 102. See also 2019 EPM at 96 (same requirement). You do not directly address this problem but seem to believe that responding to MCRC's request to confirm that Maricopa is complying with Arizona law somehow entails “[discussing our clients' election-related security operations with [MCRC][which] could compromise the ability of our clients to ensure the security of its election administration.” With all due respect to you, I don't think that is a

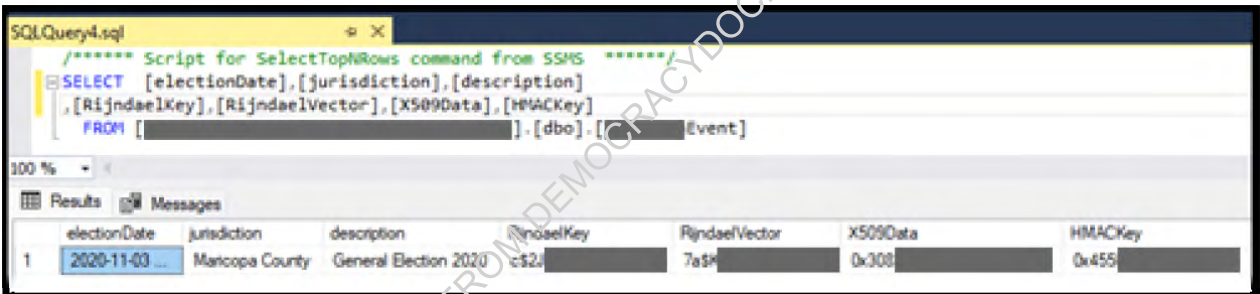


WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —

Sept. 28, 2024
Page 2 of 5

satisfactory response to a real concern. I am happy to try to work with you to address any such concerns asap. If you are still not willing, you leave us no choice.

As you know, Maricopa’s election system employs encryption keys supplied by the vendor, Dominion Voting Systems (“Dominion” or “DVS”). As shown in the redacted screenshot below taken from Maricopa’s 2020 election database these encryption keys were also surprisingly stored unprotected and in plain text in violation of the Election Assistance Commission’s (“EAC”) certification requirements. Again, for the benefit of our electorate, we urge you to address this directly and on the merits or again you leave us no choice but to do something about this.



As you also know, these vendor supplied encryption keys allow Dominion—and anyone with licit or illicit access to Maricopa’s voting system—to *e.g.*, alter or fabricate election results and unencrypt tabulator passwords on Maricopa’s voting system. These vendor supplied encryption keys are the functional equivalent of a master password because they control access to Maricopa’s election data and passwords. [REDACTED]

[REDACTED]

[REDACTED] All of these aforementioned acts plainly violate Arizona law. I don’t understand why you would not assist in addressing this serious concern.

Second, you state that “all tabulators that will be used in the 2024 general election (including the spares held in reserve) will undergo pre-election logic and accuracy testing.” Your statement fails to state that the election software to be used in the 2024 election will *also* be installed on those tabulators for the official L&A test currently scheduled on or about October 7, 2024. A.R.S. § 16-449(A) governing logic and accuracy testing and plainly requires “the automatic tabulating equipment *and* programs [be] tested to ascertain that the equipment and programs will correctly count the votes cast for all offices and on all measures.” Thus, it is a violation of A.R.S. § 16-449(A) to certify L&A testing



Sept. 28, 2024
Page 3 of 5

performed on vote center tabulators *without the election software* being that will be used on Election Day. Once again, rather than take this as some hostile demand, it is designed to assist in the integrity of the election process, which I am sure you would agree is important.

As you know, in connection with the 2022 election, Maricopa admitted seven months later that it installed reformatted memory cards on all 400+ vote center tabulators *after* certifying it had conducted statutorily required L&A testing on October 11, 2022. Hence, a real and legitimate concern arose giving rise to Mr. Olsen's letter. Maricopa claimed this was purportedly due to a mistake in the election software programming that Maricopa claimed to have discovered the day prior to the L&A test. However, as you know, Maricopa's subsequent analysis of Maricopa's tabulator logs files from the 2020 general election show Maricopa apparently did the same thing in connection with the 2020 election. Putting aside the questions this raises about Maricopa's purported excuse for having to install reformatted memory cards into the vote center tabulators used in the 2022 election, this indicates Maricopa has a practice of installing reformatted memory cards with election software *after* the official L&A test date without performing L&A testing on those tabulators in accordance with A.R.S. § 16-449. Again, a legitimate concern that requires it being addressed now.

Third, Maricopa employed altered election software in the 2020 and 2022 elections that was not approved for use in Arizona in accordance with A.R.S. § 16-442, and falsely represented that it used DVS Democracy Suite 5.5B election software certified by the EAC, including that the hash values matched with the certified software. As shown in an exemplar tabulator log file produced by Maricopa and shown below, the configuration file governing machine behavior settings ("MBS") is of a different DVS software version (Democracy Suite 5.10), not approved by the Arizona Secretary of State, has been grafted onto Maricopa's Democracy Suite version 5.5B election software. Again, this a very legitimate concern and issue raised that needs a concerned response. Sloughing this off will not be acceptable, nor should it be.

```
10248_A_SLOG.TXT X
runtime settings started
14 Oct 2022 11:37:30 [ProjectVerifier] WARN : [Verification] Wrong mbs version: 5.10.9.4
Expecting: 5.10.3.4
14 Oct 2022 11:37:30 [ProjectVerifier] INFO : [Verification] Loading conditional points from
alternative selectors
```



Sept. 28, 2024

Page 4 of 5

The MBS are a critical software component governing how a voter's ballot is read and tabulated. The MBS file could not have been produced by the DVS version 5.5B. The election software Maricopa County used in the November 2020 and November 2022 elections has been materially altered from the EAC and Arizona Secretary of State certified.

Maricopa's violations of Arizona law go to the heart of the integrity of its electronic voting machines, and voter confidence in their accuracy and reliability. In light of the aforementioned repeated and deliberate violations of law, on behalf of the MCRC, we again respectfully ask that Maricopa confirm the following in writing by the close of business Wed., October 2, 2024:

1. Maricopa's election systems no longer employ *any* vendor-supplied passwords, including any vendor-supplied encryption keys, as mandated by the EPM.
2. Maricopa's current passwords can only be known by authorized users, as mandated by the EPM, and cannot be decrypted by any encryption key known by DVS or decrypted or derived by any unauthorized user.
3. DVS Democracy Suite version 5.17, as approved by the Arizona Secretary of State in accordance with A.R.S. § 16-442, has been installed on all Maricopa election systems and components (including the EMS, all ICP2 and ICC tabulators, and all components used, including ballot marking devices).
4. The election software Maricopa used in the 2020 and 2022 elections, and any software not approved by the Arizona Secretary of State does not now reside on any of these components identified above, nor on any removable media in Maricopa's possession or accessible to any person or office with physical access to Maricopa voting systems.
5. After the completion of the official statutorily announced and compliant L&A test scheduled to take place on or about October 7, 2024, Maricopa will *not* reformat or alter the L&A tested software configuration on any memory cards of any tabulator, or install any election software on any tabulator, without conducting a statutorily compliant L&A test on those tabulators in accordance with A.R.S. § 16-449 after taking such actions. If you believe L&A testing the tabulators independently of L&A testing the election software complies with A.R.S. § 16-449, please state that in writing and the basis for that belief.



WILENCHIK & BARTNESS

— A PROFESSIONAL CORPORATION —

Sept. 28, 2024

Page 5 of 5

If we do not receive a specific response to these simple requests by the close of business on Wednesday, October 2, 2024, the MCRC will be left with no other choice but to pursue litigation to compel Maricopa County provide such assurances so as to prevent Maricopa from repeating its prior violations of Arizona election law. Joe, I just want to add that I do not write this in a threatening manner and hopefully you will not take it that way. However, I do not know what else to do to assure our client of the integrity of the process and hope you will see it that way and be cooperative. If not, please tell me why you cannot do so and maybe we can discuss before I have to take action. My best personal regards to you and your colleagues there.

Sincerely Yours,

A handwritten signature in black ink, appearing to read 'Dennis I. Wilenchik', written in a cursive style.

Dennis I. Wilenchik

RETRIEVED FROM DEMOCRACYDOCKET.COM

EXHIBIT 6

RETRIEVED FROM DEMOCRACYDOCS.COM

WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —



Maricopa County Attorney

RACHEL MITCHELL

October 3, 2024

VIA EMAIL ONLY

Dennis Wilenchik, Esq.
Wilenchik & Bartness
2810 N. Third Street
Phoenix, AZ 85004

RE: Your September 28, 2024, letter on behalf of the MCRC

Dear Dennis:

We received your letter of September 28, 2024 (the “Letter”), which you sent on behalf of your client, the Maricopa County Republican Committee (the “MCRC”). The Letter contained several inaccurate statements about Maricopa County’s election practices and procedures, which were based on the incorrect assumptions and erroneous conclusions of Kurt Olsen’s so-called “experts.” The Letter also alluded to a possible lawsuit, which you might bring on behalf of the MCRC, if we did not assuage your concerns that Maricopa County might “repeat[] its prior violations of Arizona election law.” And it made five demands.

To be clear, the allegations contained in the Letter are false, as will be explained below. And none of your demands are warranted. The County will follow the law, as it always does, and will not accede to your client’s demands that are not supported by the law.

PREFATORY STATEMENT

To be crystal clear, Maricopa County has **not** violated Arizona election law. Neither has the Recorder. And neither has the Elections Department.¹ The allegations to the contrary, made by Kurt Olsen and his so-called “experts” Clay Parikh and Ben Cotton, are false and defamatory.² As

¹ For the remainder of this response letter, Maricopa County, the Recorder, and the Elections Department will be jointly referred to as the “County.”

² Arizona courts have recognized the litigation privilege against being held accountable for defamatory statements made *in judicial proceedings*. See, e.g., *Green Acres Tr. v. London*, 141 Ariz. 609, 613-15 (1984). However, no such privilege exists for statements made outside of the

attorneys, you and Mr. Olsen have a duty not just to advocate for your client, but “avoid causing injury to [your] opponents” by “treat[ing] with consideration all persons involved in the legal process and to avoid the infliction of needless harm.” *Green Acres Tr. v. London*, 141 Ariz. 609, 615 (1984) (quoting The Model Code of Professional Responsibility (1979)). Further, Rule 11 of the Rules of Civil Procedure **require attorneys to make a “reasonable inquiry” into any factual contentions made in a Complaint** before signing it; and, the attorney’s signature certifies that “to the best of [the attorney’s] knowledge, information and belief formed after reasonable inquiry ... the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery[.]” Ariz. R. Civ. P. 11(b)(3); *see also* Fed. R. Civ. P. 11(b)(3) (substantively the same).

The County has litigated, and won, a multitude of challenges to its elections and election practices and procedures since Donald Trump’s defeat in the 2020 general election. Many of those were arguably frivolous lawsuits. *See, e.g., Bowyer v. Ducey*, 506 F. Supp. 3d 699 (D. Ariz. 2020) (ruling that “[p]laintiffs failed to provide the Court with factual support for their extraordinary claims” and, in any event, “wholly failed to establish that they have standing for the Court to consider them.”)³ But the County is not in the habit of seeking sanctions against opposing litigants and their attorneys, even when the litigation is arguably frivolous. Still, on three occasions, the County has thought the litigation to be so obviously frivolous that sanctions should be pursued. Kurt Olsen was the opposing counsel for each of those three lawsuits.

The County successfully obtained sanctions against Mr. Olsen when he brought a lawsuit making similar allegations against the County’s Dominion Voting Systems equipment as he (and you)

proceedings and to persons who have no relation to the proceedings, such as defamatory statements made via social media. *Id.*

³ Plaintiffs in the *Bowyer v. Ducey* litigation alleged “that Arizona’s Secretary of State and Governor conspired with various domestic and international actors to manipulate Arizona’s 2020 General Election results allowing Joseph Biden to defeat Donald Trump in the presidential race.” *Bowyer*, 506 F. Supp. at 721. But the Court noted that plaintiffs presented no evidence to support that extraordinary claim. They submitted expert reports, but “the ‘expert reports’ reach implausible conclusions, often because they are derived from wholly unreliable sources.” *Id.* at 722 (quotation marks around “expert reports” in original). Plaintiffs submitted “over three hundred pages of attachments, which are only impressive for their volume.” *Id.* at 721. “The various affidavits and expert reports are largely based on anonymous witnesses, hearsay, and irrelevant analysis of unrelated elections.” *Id.* And “[t]he Complaint is equally void of plausible allegations that Dominion voting machines were actually hacked or compromised in Arizona during the 2020 General Election.” *Id.* at 723. The Court admonished that “[a]llegations that find favor in the public sphere of gossip and innuendo cannot be a substitute for earnest pleadings and procedure in federal court.” *Id.* at 724.

Despite the frivolous nature of this lawsuit, the County did not seek sanctions.

make in the Letter. *Lake v. Hobbs*, 623 F. Supp. 3d 1015 (D. Ariz. 2022), *aff'd sub nom. Lake v. Fontes*, 83 F.4th 1199 (9th Cir. 2023), *cert. denied*, 144 S. Ct. 1395 (2024). The court “held that speculative allegations that voting machines may be hackable are insufficient to establish an injury in fact under Article III.” *Id.* at 1029. In that litigation, as here, Mr. Olsen relied on so-called “experts” for support in bringing that lawsuit, but those “experts” and their “analysis” did not impress or persuade the court. Rather, the court found for the County and the other defendants and granted the County’s request for sanctions against Mr. Olsen and his co-counsel. *Lake v. Hobbs*, 643 F. Supp. 3d 989 (D. Ariz. 2022).⁴

Additionally, our Supreme Court sanctioned Mr. Olsen for making an “unequivocally false” representation to the Court. [Exhibit 1, *Lake v. Hobbs*, No. CV-23-0046-PR, Ariz. S. Ct. (Order May 4, 2023) at 5.] Specifically, the Arizona Supreme Court ruled that “[b]ecause Lake’s attorney [*i.e.*, Kurt Olsen] has made false factual statements to the Court, we conclude that the extraordinary remedy of a sanction under ARCAP 25 is appropriate.” [*Id.*]

As will be demonstrated below, each of Kurt Olsen’s allegations against the County are false. We are providing you with this information, Dennis, so that you can correctly judge whether to participate with Mr. Olsen in what will amount to another frivolous lawsuit—one that will likely be sanctionable. We sincerely hope that you will not move forward with this threatened lawsuit. If you do, however, bring the threatened lawsuit based on the allegations made in the Letter, please be advised that the County reserves its right to seek sanctions against the plaintiff and all attorneys representing it.

I. Response to the Allegations Concerning Encryption Keys.

A. The County Only Uses County-Generated Passwords to Conduct Elections.

In the Letter, you allege that “Maricopa’s election system employs encryption keys supplied by the vendor, Dominion Voting Systems (“Dominion” or “DVS”).” [Letter at 2.] From that starting point, you allege that the County is violating the requirement, in the Elections Procedures Manual (the “EPM”), that “passwords [must] not be a vendor-supplied password and must only be known by authorized users.” [*Id.* (*quoting* EPM (2023) at 102).] This allegation is false.

Encryption keys are not passwords. They are different than passwords and have a different function. They are machine generated, which is an industry best practice, and are not something that the County can generate or control. A password, on the other hand, is an authentication that is often adjusted based off of a user account and can be set by the owner of the system. The County can, and does, control these. Anyone with a basic understanding of information technology (“IT”)

⁴ The Ninth Circuit Court of Appeals affirmed the trial court’s decision on the merits. *Lake v. Fontes*, 83 F.4th 1199 (9th Cir. 2023), *cert. denied*, 144 S. Ct. 1395 (2024). Mr. Olsen and his co-counsel also appealed the sanctions award, and that matter is still pending on appeal.

would know this distinction, and the fact that Mr. Olsen’s so-called “experts” do not know it (or, perhaps, have chosen to ignore it) demonstrates both their inadequacy to serve as experts and also the foolishness of relying upon them and their opinions for IT and systems analysis.

You allege in the Letter that the encryption keys are “the functional equivalent” of passwords. [Letter at 2.] They are not, as any IT expert worth his salt would know. And the EPM is silent about encryption keys, and its requirements about passwords cannot be applied to them. Had the Arizona legislature wished to pass laws about encryption keys, it would have done so. And if the Secretary of State had wished to promulgate rules about encryption keys, he would have done so. Neither the legislature nor the Secretary of State did. The County complies with the EPM’s requirements concerning passwords, and there is simply no requirement in the EPM concerning encryption keys.

That the EPM is silent about vendor-generated encryption keys is not surprising. These keys are not used by the counties that administer Arizona’s elections to secure those elections. Rather, the counties, including Maricopa, use *passwords* for security purposes. The passwords used by Maricopa County are generated by the *County*, not the vendor, and are known only by authorized users.

As just stated, the County controls the passwords used to conduct elections on its Dominion Voting Systems equipment. The County does **not** use vendor-supplied passwords but creates its own unique passwords for use on the Dominion Voting Systems equipment. The County also changes its passwords before every election. And the passwords are known only to the authorized users. This means that the County is in complete compliance with the requirements of the EPM, and any allegation to the contrary is false and defamatory.

B. The County’s Election Equipment is Fully Certified and In Compliance With Its Certification.

The Letter also alleges that encryption keys are stored in “plain text,” and that this violates the Election Assistance Commission’s certification requirements. [Letter at 2.] This allegation is also false.

The Voluntary Voting System Guidelines (“VVSG”) 1.0 (2005), established by the Election Assistance Commission (the “EAC”), did not require encryption on voting systems. The VVSG 1.0 (2005) was the standard used by the EAC to certify the Dominion Democracy Suite 5.5B, which is the system that Maricopa County uses. *See* United States Election Assistance Commission, Democracy Suite 5.5B Modification (January 2, 2024), available at <https://www.eac.gov/voting-equipment/democracy-suite-55b-modification> (noting the history of the Democracy 5.5B certification process, and that the VVSG 1.0 was the applicable testing standard for its certification).

Since there was no encryption requirement in the VVSG 1.0, there was also no requirement regarding how encryption keys should be stored. Stated differently, there was no requirement that encryption keys be stored in plain text, or not stored in plain text. The VVSG 1.0 (2005) is silent on the subject.

In 2019, *after* the EAC had certified the Dominion Democracy Suite 5.5b for use in elections in the United States of America, the EAC issued an update to the VVSG, referred to as VVSG 2.0. Those new guidelines do have requirements concerning encryption for any voting systems certified pursuant to *those* guidelines (which the Dominion Democracy Suite 5.5b was *not*). But importantly, the VVSG 2.0 did not apply retroactively to systems, like the Dominion Democracy Suite 5.5b, that had already obtained certification. Rather, they remained subject to the guidelines under which they had been certified.⁵

The current version of the Dominion Democracy Suite used by the County is version 5.17, which is a modified version of Democracy Suite 5.5 through 5.5D, including 5.5B. It is fully certified by the EAC. U. S. Election Assistance Commission, Certificate of Conformance (March 16, 2023), available at https://www.eac.gov/sites/default/files/voting_system/files/D-Suite%205.17%20Certificate%20and%20Scope%20SIGNED.pdf. Version 5.17, however, is still subject to the VVSG 1.0 standard, because it is a modified version of the Democracy Suite 5.5B edition, and the VVSG 1.0 was the standard in place when the Democracy Suite 5.5B was certified in 2019. *See* Certificate of Conformance at 1 (noting that “[t]he voting system identified on this certificate has been evaluated at an accredited voting system testing laboratory for conformance to the Voluntary Voting System Guidelines Version 1.0 (VVSG 1.0)”). So, there is no requirement that the Dominion Democracy Suite 5.5B used by the County not store encryption keys in plain text, and the County’s election equipment and system is therefore **not** out of compliance with its certification. Your allegations to the contrary, made in the Letter, are false.

C. The County Does not Use Dominion-Generated Passwords to Conduct Elections.

In the Letter, you also allege that Dominion inserted “common” usernames and passwords into its voting systems. [Letter at 2.] The County knows nothing about this and so can say nothing conclusively. However, the County thinks that it is likely that the passwords you reference in the Letter—assuming that they actually exist, and that Kurt Olsen’s so-called “experts” have not merely misunderstood the data—are Dominion administrative passwords that Dominion uses to update core functionality of the EMS applications and services, much as Microsoft has Microsoft-specific authenticators built into their operating systems. Regardless, these passwords are not used by the County to administer elections or for any other function, and these passwords that you have identified cannot be used to alter election files or manipulate election data. The passwords that

⁵ Despite the VVSG being issued in 2019, no voting system has yet been certified pursuant to it. Thus, no voting system in use in United States elections is currently subject to the requirement that encryption codes not be stored in plain text.

the County uses for election purposes are unique, created by the County for each specific election, and the County does not use Dominion-generated passwords to administer its elections.

D. The Storage of Encryption Codes Presents No Security Risk.

An additional point about the encryption keys is in order, however. The fearmongering engaged in by Mr. Olsen related to the encryption keys being stored in plain text is unwarranted. Stated plainly, the storage of the encryption keys in the Election Management System (the “EMS”) server in plain text does not present a security risk. Although it is not necessary for the County to prove that fact to defeat your false allegation that the Dominion Democracy Suite 5.5B has violated its certification requirements, the County still wishes to provide a brief response to Mr. Olsen’s fearmongering.

First, and importantly, the tabulators in vote centers do not store the encryption keys in plain text. Rather, with the 5.17 upgrade to the Dominion Democracy Suite 5.5B, the encryption keys are stored in plain text *only* on the EMS server, and new encryption keys are machine generated by the Dominion system for each election. So, if someone had an encryption key from a previous election, it would not work for the current election. The old encryption keys, which Mr. Olsen’s so-called “experts” claim to have, are useless.

The EMS server is housed in the EMS Server Room, which is a secure room with transparent walls made of see-through glass or similar material. The EMS server is fully air-gapped and so is not connected to the Internet or any outside source. Consequently, the only way to gain access to the EMS server is through in-person, physical contact.

Additionally, the EMS hard drives are encrypted, and the encryption keys discussed in your Letter, residing in plain text on the EMS server, will not “de-encrypt” those hard drives. Rather, in layman’s terms, the encryption is different and those encryption keys are not able to access the hard drives.

The EMS Server Room is locked at all times, and only a small number of authorized County employees have keycards that will access it. It is housed within the Ballot Tabulation Center (the “BTC”), which also requires key card access. Further, the BTC and the EMS Server Room are under video surveillance twenty-four hours a day, seven days a week; and, that video feed is livestreamed to the world, so that anyone with Internet access who wants to watch the BTC and EMC server room can do so.

The BTC, meanwhile, is located inside the Maricopa County Tabulation and Election Center (“MCTEC”), which is one of the most secure buildings in Maricopa County.

In order to gain access to the encryption keys and possibly be able to somehow affect an election, one would have to gain access to the EMS server. This would require a bad actor to break into MCTEC, then into the BTC, then into the EMS Server Room, then successfully “de-encrypt” the

EMS hard drives, then take several more steps that I will not mention in this letter for purposes of maintaining security—all while not being detected or caught in a multitude of different ways that will also not be discussed here.

This is simply not a realistic possibility. The fearmongering over this is irresponsible, and it needs to stop.

II. Response to the Allegations Concerning Logic and Accuracy Testing.

On pages 2 through 3 of the Letter you make numerous allegations about the logic and accuracy (“L&A”) testing of the County’s machines in prior elections. The allegations betray a serious misunderstanding of what actually occurred. This has all been stated previously; it is a little surprising that Mr. Olsen is still misrepresenting it. Nonetheless, the County will once again explain what happened, which demonstrates that Mr. Olsen’s allegations to the contrary are false.

In 2022, the County performed L&A testing on 100% of its tabulators before each election, including the 2022 general election. This is a separate L&A test from the Secretary of State’s L&A testing, and is also separate from the County’s additional L&A testing conducted on the same day as the Secretary’s L&A testing. Contrary to what some have falsely claimed, in this first County L&A testing, 100% of the tabulators that will be used in the upcoming election (including all of the tabulators held in reserve as “spares” for that election) are subjected to L&A testing.

During the final part of the County’s L&A test of 100% of its tabulators and prior to the Secretary of State’s L&A testing, the County discovered that the Election Program was not configured to cause the tabulators in the voting locations (commonly called “precinct-based tabulators”) to reject early ballots and provisional ballots. Neither the EPM nor the Arizona statutes require the Election Program to be so configured. But the County recognizes that it is a “best practice” to prevent the precinct-based tabulators to “read” early ballots and provisional ballots, in order to help prevent the possibility of someone casting two ballots by inserting them both into the tabulator (for example, a ballot they were issued in the voting location and also an early ballot that they received in the mail). Once the County discovered that the Election Program was not configured in accordance with the way the County thinks is the best practice, the County added this best-practice protocol to the Election Program. The Election Program, with this added protection, then was loaded onto the tabulators that were randomly selected for the statutorily-required Secretary of State’s L&A, as well as the County’s L&A additional test conducted the same day as the Secretary’s. The central count tabulators, the randomly selected precinct-based tabulators and the program that was installed on 100% of all tabulators, passed that testing. After the County’s 2022 General Election program passed L&A testing and was certified for use, the County removed the memory cards from the tabulators that were not selected for the random testing and installed memory cards containing the certified Election Program with the added protection the County applied, which had just passed the Secretary’s and County’s L&A testing, into those tabulators.

The County then performed additional testing on 100% of the County's tabulators with the Election Program with the added protection installed, which—once again—the tabulators and Election Program passed.

All of this was done under the live stream cameras and could be viewed by anyone in the world with access to the Internet.

As for your allegations about L&A testing in 2020, the County does not know to what you are referring. The County is not aware of any analysis that the County did that shows that the same thing occurred in 2020, as you allege on page 3 of the Letter.⁶

III. Response to Allegations Concerning the Dominion Democracy Suite Software Used by the County.

In the Letter, on page 3, you incorrectly claim that “Maricopa employed altered election software in the 2020 and 2022 elections that was not approved for use in Arizona in accordance with A.R.S. § 16-442, and falsely represented that it used DVS Democracy Suite 5.5B election software certified by the EAC, including that the hash values matched with the certified software.”

This allegation is false, and demonstrates either the lack of understanding of Kurt Olsen's so-called “experts” of voting systems technology or their inability to analyze data that is right in front of their faces. Either way, the allegation demonstrates that the opinions of these so-called “experts” cannot be relied upon.

To state the matter clearly and plainly, the County used the Dominion Democracy Suite 5.5B software in the 2020 and 2022 elections. This software, including its minor version 5.10.X.X, was certified and approved by the EAC for use in elections in the United States, and then certified and approved by the Arizona Secretary of State for use in Arizona, in 2019. All of this satisfied the requirements of A.R.S. § 16-442. At no time has the County misrepresented these facts, which are easily verifiable with the “reasonable inquiry” required by Rule 11.

All the Dominion central count and precinct tabulators used by Maricopa County during the 2020 and 2022 General Elections met federal and state certification requirements and were fully compliant with the EAC and its VVSG 1.0 standards. This includes the Dominion Voting Systems (DVS) Democracy Suite (D-Suite) Election Management System (EMS) version 5.5B (Certified on August 21, 2019), as well as the certified ICP2 firmware version 5.5.1.8. See print screen below

⁶ You write, “However, as you know, Maricopa's subsequent analysis of Maricopa's tabulator logs files from the 2020 general election show Maricopa apparently did the same thing [presumably, “install[ing] reformatted memory cards”] in connection with the 2020 election.” The County is not aware of what analysis to which you refer and further does not recall any such showing by Maricopa County or anyone else.

from the [Dominion Voting Systems D-Suite 5.5-B Test Plan-Rev. 03 28As run 29.pdf](#) section 2.2.1.1 page 17.

Addition of ImageCast Precinct 2 (ICP2) optical ballot counter. The ICP2 is a precinct-based optical scan ballot tabulator that is used in conjunction with ImageCast compatible ballot storage boxes. **Submitted version: ICP2 firmware version 5.5.1.8, model number PCOS-330A.**

The Letter includes a print screen from the 10248_A_SLOG.TXT. We have provided additional lines from the same SLOG file that demonstrates the Image Cast Precinct 2 tabulators have the certified version installed as reference in the Dominion Democracy Suite 5.5B test plan.

```

01 Jan 1970 00:00:10 [Main thread] INFO : [Init] Logging service initialized, starting ImageCastPrecinct v 5.5.1.8
01 Jan 1970 00:00:10 [Main thread] INFO : [Init] CentralManager activated
01 Jan 1970 00:00:10 [Main thread] INFO : [Thermal Printer] Turn off printer power
01 Jan 1970 00:00:10 [Main thread] INFO : Machine serial number: VAL21520119
01 Jan 1970 00:00:10 [Main thread] INFO : [Power Controller] Power Controller FW Version: 0.0.27
01 Jan 1970 00:00:10 [Main thread] INFO : [Power Controller] Coin battery voltage: 3201mV
14 Oct 2022 11:36:20 [Main thread] INFO : Lifetime counters read from EEPROM: total cast 43, forwarded 38, diverted 5
14 Oct 2022 11:36:24 [Main thread] INFO : [Init] Adding Translator Bengali File: /media/system-card-data/data/Translations/Bengali.qm
14 Oct 2022 11:36:24 [Main thread] INFO : [Init] Adding Translator Chinese File: /media/system-card-data/data/Translations/Chinese.qm
14 Oct 2022 11:36:24 [Main thread] INFO : [Init] Adding Translator English File: /media/system-card-data/data/Translations/English.qm
14 Oct 2022 11:36:24 [Main thread] INFO : [Init] Adding Translator Filipino File: /media/system-card-data/data/Translations/Filipino.qm
14 Oct 2022 11:36:24 [Main thread] INFO : [Init] Adding Translator HaitianCreole File: /media/system-card-data/data/Translations/HaitianCreole.qm
  
```

Additionally, the EAC test documentation includes a table of Machine Behavior Settings (MBS) that were tested and certified. [[Dominion Voting Systems D-Suite 5.5-B Test Plan-Rev. 02.pdf](#) Table 4-2. Test Development Plan Documents line 1 page 31]. See print screens below that show a minor version number of 5.5-B::10 that was included in the EAC test documentation.

Table 4-2. TDP Documents (continued)

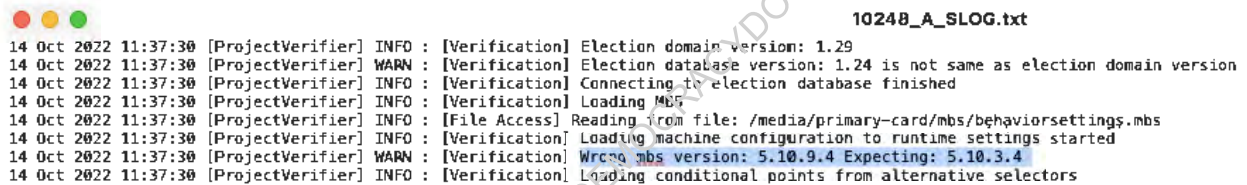
Document Number	Description	Version
---	Democracy Suite ImageCast Precinct 2 Machine Behavior Settings	5.5-B::10
---	APC Smart-UPS 1500 Specification Sheet	---
---	Democracy Suite ImageCast Precinct 2 Extracting Firmware	---

The test document and the print screen on the prior page include the MBS version 5.5-B::10. The double colon “::” in the version number is a wildcard. Application developers across technology platforms use wildcards symbols like * or :: when created documentation in version control systems to manage and reference a range of versions. Wildcards, often represented by symbols like *, X, or ::, allow developers to specify version ranges without explicitly naming each minor version number. For example, developers might use wildcards to indicate compatibility with all minor or patch versions of a library, such as 1.2.*, which would match any version 1.2.X.X. This

conforms with the primary version displayed in the “10248_A_SLOG.txt” file, which you included in the Letter on page 3, as 5.10.X.X (*i.e.*, 5.10.9.4 and 5.10.3.4).

DVS distinguishes between versions as either a “major version” or “minor version”. The major version is the overall system identifier that is listed as the version number (*e.g.*, Democracy Suite 5.5B). The minor versions are application or configuration versions such as machine behavior settings (MBS) files. The Dominion Democracy Suit 5.5B included a range of minor versions that were also certified in 2019.

MBS version 5.10.9.4 is an MBS minor version of the certified “5.5-B::10” version and conforms with required standards, including being certified at the federal and state level during the certification of Democracy Suite 5.5B in 2019. This message, below, does not indicate an invalid or uncertified MBS minor version, but a minor version that is an expected configuration when running a validation check.



```
10248_A_SLOG.txt
14 Oct 2022 11:37:30 [ProjectVerifier] INFO : [Verification] Election domain version: 1.29
14 Oct 2022 11:37:30 [ProjectVerifier] WARN : [Verification] Election database version: 1.24 is not same as election domain version
14 Oct 2022 11:37:30 [ProjectVerifier] INFO : [Verification] Connecting to election database finished
14 Oct 2022 11:37:30 [ProjectVerifier] INFO : [Verification] Loading MBS
14 Oct 2022 11:37:30 [ProjectVerifier] INFO : [File Access] Reading from file: /media/primary-card/mbs/behaviorsettings.mbs
14 Oct 2022 11:37:30 [ProjectVerifier] INFO : [Verification] Loading machine configuration to runtime settings started
14 Oct 2022 11:37:30 [ProjectVerifier] WARN : [Verification] Wrong mbs version: 5.10.9.4 Expecting: 5.10.3.4
14 Oct 2022 11:37:30 [ProjectVerifier] INFO : [Verification] Loading conditional points from alternative selectors
```

This is something that a true IT expert who had familiarity with SLOG file analysis would know. To be clear, the MBS identifier 5.10.9.4 does not indicate that the County altered the Democracy Suite 5.5B software, as Kurt Olsen’s so-called “experts” appear to believe. In the Letter, you claim that this “forensic evidence conclusively demonstrat[es] Maricopa’s violations of election law.” [Letter at 1.] But the reality is that the evidence proves that the County’s election equipment made use of the 5.10 minor version, which had been certified as part of the Democracy Suite 5.5B in 2019. This demonstrates that the County **was complying** with applicable election law, not violating it. It is fine that you and I do not know that; we are attorneys, not IT experts, and do not claim to be. Kurt Olsen’s so-called “experts,” however, hold themselves out as experts in this field. But they either do not understand the data or else they are misrepresenting what it reveals. Either way, neither they nor their opinions should be relied upon when crafting a Complaint (nor when conducting the requisite Rule 11 “reasonably inquiry”). To be clear, there was nothing wrong with the demonstrative that you included on page 3 of the Letter. The problem lies with Olsen’s so-called “experts.”

To continue: the assertion made in the Letter, on page 3, that the MBS minor version 5.10.9.4 “could not have been produced by the DVS version 5.5B,” is incorrect. As described above, the MBS file 5.10.9.4 is included in range of EAC certified MBS files and the programming of the ICP2 device SD cards used in the precinct-based tabulators can only be done within an EAC certified DVS D-Suite 5.5B environment due to EAC and VVSG 1.0 required cyber and physical security controls. This programming is only performed by County’s staff, in the BTC within the

MCTEC facility. The SD cards, with the certified applications and configurations, are installed in the ICP2 devices (*i.e.*, the precinct-based tabulators), within that same secured room under surveillance cameras and access control by authorized personnel. The SD cards are then secured using serialized tamper evident seals before leaving the BTC. Those seal numbers are documented and auditable. Any indication of tampered seals would launch an investigation and subsequent equipment audits.

Furthermore, the ICP2 devices (*i.e.*, the precinct-based tabulators) were tested and confirmed, prior to and after the 2020 and 2022 General elections, by post-election L&A testing conducted by both the County and the Secretary of State. The tabulation by the County’s tabulators was also confirmed by post-election, bi-partisan hand-count audits. If the MBS minor version numbers were detrimental to the operation of the precinct-based tabulators, they would not have passed L&A testing and hand count audits.

In 2024, Maricopa County Elections upgraded from the DVS D-Suite 5.5B major version application to the EAC certified DVS D-Suite 5.17 major version. DVS D-Suite 5.17 was certified by the EAC on March 16, 2023 and approved by the Arizona Secretary of State’s office on May 25, 2023. *See* United States Election Assistance Commission, Certificate of Conformance (March 16, 2023), available at https://www.eac.gov/sites/default/files/voting_system/files/D-Suite%205.17%20Certificate%20and%20Scope%20SIGNED.pdf; Arizona Secretary of State Certified Vote Tabulating Equipment (January 18, 2024), available at https://azsos.gov/sites/default/files/2024-02/2024_0118_Official_Voting_Equipment_List.pdf.

As demonstrated by the inclusion of the attached links, the certification of the County’s Dominion Voting System equipment is easily discoverable, and should have been discovered by Kurt Olsen’s so-called “experts.” That they apparently did not is troubling.

In the EAC certification filing documents, Dominion describes the relationship between major versions 5.5B and 5.17, “The D-Suite 5.17 Voting System configuration is a modification from the EAC approved D-Suite 5.5-D system configuration.” [[D-Suite 5.17 Certificate and Scope SIGNED.pdf](#) page 1]. The EAC documentation lists all major and minor system changes between version 5.5B and 5.17. The major version identifier is 5.17.X.X and the identified ICP2 firmware minor version is 5.17.15.1. The MBS minor version is 5.17.8.1_EAC_5.17_20220 727, which corresponds to the version listed in the SLOG files of a test ICP2 with DVS D-Suite 5.17 installed. [[D-Suite 5.17 Certificate and Scope SIGNED.pdf](#) page 9].

File Name	Version	Access	Location
Machine Configuration File (MCF)	5.17.15.1_20220920	Proprietary	ICX Configuration File
Device Configuration File (DCF)	5.17.9.1_20220916	Proprietary	ICP and ICC Configuration File
ICE Machine Behavior Settings	5.17.8.1_EAC_5.17_20220 727	Proprietary	ICE Configuration
ICP2 Machine Behavior Settings	5.17.8.1_EAC_5.17_20220 727	Proprietary	ICP2 Configuration

The S-LOG or “SLOG” file is a text-based log from ICP2 devices (*i.e.*, precinct-based tabulators) that contains configuration information, machine behavior and event descriptions. In a test

deployment for the DVS D-Suite 5.17 on an ICP2 machine, the SLOG files have matching major and minor version numbered software and MBS files. There is simply nothing incorrect about the County's Dominion Voting System equipment's SLOG file data, and the Letter's assertions to the contrary are false.

IV. Responses to the Letter's "Demands."

On page 4 of the Letter, you make a series of "demands" that the County must meet in order to avoid you filing a lawsuit on behalf of the MCRC. I hope that what I have written, above, has caused you to rethink the wisdom of your proposed lawsuit. I also, however, want to respond to each of your demands.

First, you demand that the County confirm in writing that its election systems will not utilize any vendor-supplied passwords, "including vendor-supplied encryption keys, as mandated by the EPM." As already explained, the County does not use vendor-supplied passwords; rather, every password that the County uses to administer elections is County created. As such, the County is fully compliant with the EPM's requirements concerning passwords. The EPM does not have any requirements concerning encryption keys, which the County does not control anyway. As was explained, they are system generated (not created by the County). Regardless, because no law requires that the County's election equipment not use "vendor-supplied encryption keys," and the County's election equipment has passed all required certification even though it contains "vendor-supplied encryption keys" (and so, the presence of those keys is not an impediment to certification), the County will decline to adopt Kurt Olsen's policy preferences concerning encryption keys.

Second, you demand that the County confirm in writing that its current passwords can only be known by authorized users and cannot be decrypted by Dominion Voting Systems or other users. As has previously been explained, the County creates new, unique passwords for each election, and those passwords are only known by authorized users. They are not known to Dominion Voting Systems or anyone who is not an authorized user.

Third, you demand that the County confirm in writing that DVS Democracy Suite version 5.17, as approved by the Arizona Secretary of State in accordance with A.R.S. § 16-442, has been installed on all Maricopa election systems and components. As has been explained already, 5.17 is the upgrade to the Dominion Democracy Suite 5.5B system that the County uses, and it is what is installed on all of the relevant Dominion Voting Systems equipment.

Fourth, you demand that the County confirm in writing that the "election software used in the 2020 and 2022 elections, and any software not approved by the Arizona Secretary of State[,] does not now reside on" any of the County's election equipment. This is somewhat of a nonsensical demand. That said, no software "not approved by the Arizona Secretary of State" resides on the election equipment. The Democracy Suite 5.5B, which the County has used in every election since it was first used in 2019, including the 2020 and 2022 elections, *does* continue to reside on the

County's equipment, because the 5.17 upgrade almost certainly contains components of it. Stated differently, the 5.17 upgrade is still the Democracy Suite 5.5B system. What is more, there would be nothing unlawful for the County to choose to use the 5.10 minor revision, which it previously used. The County has chosen to use the 5.17 upgrade, but it is not required to do so. Regardless, your demand that the County remove its election operating system is baffling. The 5.5B system (which included the 5.10 minor revision) has been certified, as has the 5.17 upgrade, and the County will use the 5.17 upgrade in the 2024 general election, just as it used it in the 2024 primary election.

Fifth, you demand that the County confirm in writing that it will not alter the Election Program (*i.e.*, what you call the "software configuration on any memory cards of any tabulator") after the Secretary of State's statutorily-required L&A testing, or install an Election Program on any tabulator that has not passed that required testing. The County did not do this in 2022, despite your false allegation to the contrary, and will not do it in the future. As explained above, prior to the 2022 general election the County made a best-practices addition to the Election Program prior to the Secretary's L&A testing. It then installed that Election Program on the tabulators that were randomly selected for the testing in the Secretary's L&A testing and the County's additional L&A testing conducted the same day as the Secretary's. Only after passing that testing was the updated Election Program installed on the tabulators that had not been selected for that particular L&A testing.

As a reminder, your client, the MCRC, is invited each election to attend the L&A testing of the County's tabulation equipment. If it has any concerns about the testing as it is observing it, I invite you to let me know.

CONCLUDING STATEMENT

Having now addressed your concerns and answered your demands, we sincerely hope that you and your client will reconsider the litigation threatened in the Letter to us. There is no justifiable basis for such a lawsuit, and certainly no good-faith one that would meet the expectations of Rule 11.

We strongly recommend that as you complete the requisite "reasonable inquiry" required by Rule 11, you explore well beyond the repeated assertions of Messrs. Olsen, Parikh, and Cotton. If you do not trust the experts that we have relied upon to draft the more technical aspects of this response, we suggest that you contact experts from the EAC or the Secretary of State's Office. You will find that they will confirm what we have written to you in this letter.

It is our sincere hope that you and your client will distance yourself from Mr. Olsen's incorrect theories and false allegations about the County. For whatever reason, he and his so-called "experts" appear to have a vendetta against the County and its attorneys. But vendettas do not satisfy Rule 11's requirements. Rather, attorneys signing pleadings "certify[y] that to the best of [their] knowledge, information and belief formed after a reasonable inquiry[,]" that "the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary

support after a reasonable opportunity for further investigation or discovery[.]” Here, that is simply not the case. We do not want to waste judicial and taxpayer resources, as well as your client’s resources, to establish in court what we have demonstrated here in this response letter. But if your client sues our client, we will. We will bring in EAC-qualified testing laboratory experts, who will conclusively prove that Kurt Olsen’s so-called “experts” are incorrect in their assertions. We will prove as a matter of law that Arizona and federal law requires exactly what it requires, and does not require the County to adopt Kurt Olsen’s policy preferences. We will show that you and your client were told these things in advance of filing their lawsuit. And, while litigation is always uncertain and no lawyer should guarantee a result, we believe that we will prevail in the litigation because “both the facts and the law are on our side, which is a good place to be,” as the old saying goes.

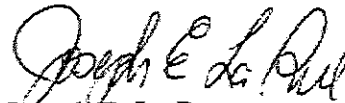
Be advised, and please advise your client, that if you and your client move forward with this litigation the County reserves its right to seek sanctions against the attorneys and parties who bring the lawsuit, as well as to seek its attorney fees and costs.

Sincerely,

RACHEL MITCHELL
MARICOPA COUNTY ATTORNEY



Thomas P. Liddy
Civil Division Chief



Joseph E. La Rue
Election Law Team Leader

RETRIEVED FROM DEMOCRACYDOCKET.COM

Exhibit 1

RETRIEVED FROM DEMOCRACYDOCKET.COM

SUPREME COURT OF ARIZONA

KARI LAKE,) Arizona Supreme Court
) No. CV-23-0046-PR
Plaintiff/Appellant,)
) Court of Appeals
v.) Division One
) No. 1 CA-CV 22-0779
KATIE HOBBS, et al.,) 1 CA-SA 22-0237
) (Consolidated)
Defendants/Appellees.)
) Maricopa County
KARI LAKE,) Superior Court
) No. CV2022-095403
)
Petitioner,)
) **FILED 05/04/2023**
v.)
)
THE HONORABLE PETER THOMPSON,)
JUDGE OF THE SUPERIOR COURT OF)
THE STATE OF ARIZONA, in and for)
the County of Maricopa,)
)
Respondent Judge,)
)
KATIE HOBBS, personally as)
Contestee; ADRIAN FONTES, in his)
official capacity as Secretary)
of State; STEPHEN RICHER, in his)
official capacity as Maricopa)
County Recorder, et al.,)
)
Real Parties in Interest.)
)

ORDER

In their responses to Petitioner Lake's Petition for Review, Respondents Secretary of State Fontes and Governor Hobbs moved for sanctions against Lake and her attorneys pursuant to Ariz. R. Civ. App. P. (ARCAP) 25 and A.R.S. § 12-349 (collectively, "Motions for Sanctions"). This Court entered its Order affirming the trial court

and Court of Appeals on most issues, but reversing those courts on their dismissal of the signature verification claim on the basis of laches and remanding that issue to the trial court.

On the issue of whether votes were improperly added by a third-party vendor, we stated that “[t]he record does not reflect that 35,563 unaccounted ballots were added to the total count.” We instructed the parties to “address as a basis for sanctions only Petitioner’s factual claims in her Petition for Review (i.e., that the Court of Appeals should have considered ‘the undisputed fact that 35,563 unaccounted for ballots were added to the total [number] of ballots at a third party processing facility’).” The parties filed briefs on this issue, and Lake filed a Motion for Leave to file a motion for reconsideration of the Court’s denial of review on the chain-of-custody issue.

Candidates are free to timely challenge election procedures and results, and the public has a strong interest in ensuring the integrity of elections. Sometimes campaigns and their attendant hyperbole spill over into legal challenges. But once a contest enters the judicial arena, rules of attorney ethics apply. Although we must ensure that legal sanctions are never wielded against candidates or their attorneys for asserting their legal rights in good faith, we also must diligently enforce the rules of ethics on which public confidence in our judicial system depends and where the truth-seeking function of our adjudicative process is unjustifiably

hindered.

ARCAP 25 authorizes an appellate court to impose sanctions on an attorney if the court determines that an appeal or a motion is frivolous, and provides that “[a]n appellate court may impose sanctions that are appropriate in the circumstances of the case, and to discourage similar conduct in the future.” Other rules similarly require candor in court proceedings. See, e.g., Ariz. R. Civ. P. 11(b) (providing that “[b]y signing a pleading, motion, or other document,” an attorney “certifies that to the best of the person’s knowledge, information, and belief” that “the factual contentions have evidentiary support”); see also Ariz. R. Sup. Ct. 42, Ethical Rule (“ER”) 3.3 (“A lawyer shall not knowingly . . . make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer.”).

Under A.R.S. § 12-349(A), claims are sanctionable if they are brought “without substantial justification.” Further, “without substantial justification” means that the “claim or defense is groundless and is not made in good faith.” § 12-349(F). Groundlessness is “determined objectively,” and a claim is groundless “if the proponent can present no rational argument based upon the evidence or law in support of that claim.” *Takieh v. O’Meara*, 252 Ariz. 51, 61 ¶ 37 (App. 2021), review denied (Apr. 7, 2022) (quoting *Rogone v. Correia*, 236 Ariz. 43, 50 ¶ 22 (App. 2014)).

ARCAP 25 gives an appellate court broad authority to impose sanctions "that are appropriate in the circumstances of the case" on an attorney or a party if it determines that an appeal or motion is frivolous. This includes "contempt, dismissal, or withholding or imposing costs." ARCAP 25.

In her Complaint, Lake set forth colorable claims, including ballot chain-of-custody claims, that were rejected following an evidentiary hearing in the trial court, and she duly but unsuccessfully (except for the laches issue) challenged those rulings on appeal. However, she has repeatedly asserted that it is an "undisputed" fact that 35,563 ballots were added or "injected" at Runbeck, the third-party vendor. Not only is that allegation strongly disputed by the other parties, this Court concluded and expressly stated that the assertion was unsupported by the record, and nothing in Lake's Motion for Leave to file a motion for reconsideration provides reason to revisit that issue. Thus, asserting that the alleged fact is "undisputed" is false; yet Lake continues to make that assertion in her Motion for Leave.

Lake's Petition for Review stated that it was an "undisputed fact that 35,563 unaccounted for ballots were added to the total number of ballots at a third party processing facility." In her Opposition to Motion for Sanctions and Motion for Leave, she repeats this contention, stating that "[t]he record indisputably reflects at least 35,563 Election Day early ballots, for which there is no record

of delivery to Runbeck, were added at Runbeck,” As the Court of Appeals observed, Lake’s argument was focused on one exhibit that included an estimate of the number of early ballot packets based on the number of trays and a different exhibit showing a precise count. Although Lake may have permissibly argued that an inference could be made that some ballots were added, there is no evidence that 35,563 ballots were and, more to the point here, this was certainly disputed by the Respondents. The representation that this was an “undisputed fact” is therefore unequivocally false.¹

Because Lake’s attorney has made false factual statements to the Court, we conclude that the extraordinary remedy of a sanction under ARCAP 25 is appropriate.

The Governor and Secretary seek sanctions for attorney fees and in the Secretary’s reply he seeks additional sanctions. Because Lake prevailed in her argument that the trial court improperly found her signature verification argument barred by laches, an additional sanction is not warranted. Therefore,

IT IS ORDERED denying the Motion for Leave.

¹ See ER 3.3 Comment 2: “This rule sets forth the special duties of lawyers as officers of the court to avoid conduct that undermines the integrity of the adjudicative process. A lawyer acting as an advocate in an adjudicative proceeding has an obligation to present the client’s case with persuasive force. Performance of that duty while maintaining confidences of the client, however, is qualified by the advocate’s duty of candor to the tribunal. Consequently, . . . the lawyer must not mislead the tribunal by false statements of law or fact or evidence that the lawyer knows to be false.”

IT IS FURTHER ORDERED denying the Secretary's Motion to Strike.

IT IS FURTHER ORDERED granting the Motions for Sanctions filed by Governor Hobbs and Secretary Fontes pursuant to ARCAP 25 as to the statement in Lake's Petition for Review asserting "the undisputed fact that 35,563 unaccounted for ballots were added to the total number of ballots," and for repeating such false assertions in an additional filing in this proceeding.

IT IS FURTHER ORDERED counsel for Lake is directed to pay to the Clerk of the Supreme Court the sum of \$2,000.00 as a sanction for this conduct, jointly and severally, such payment to be made not later than ten days from the date of this order. It is further ordered that failure to timely comply with this order may result in a termination of pro hac vice status and other sanctions as appropriate.

IT IS FURTHER ORDERED denying the requests for attorney fees as sanctions.

IT IS FURTHER ORDERED that the trial court shall forthwith conduct such proceedings as appropriate to resolve the unrelated question previously remanded.

IT IS FURTHER ORDERED directing the Clerk of Court to enter the mandate forthwith.

DATED this 4th day of May, 2023.

/s/

ROBERT BRUTINEL
Chief Justice

TO:

Bryan James Blehm
Kurt Olsen
Alexis E Danneman
Abha Khanna
Lalitha D Madduri
Christina Ford
Elena Rodriguez Armenta
Shayna Gabrielle Stuart
Jake Tyler Rapp
Craig A Morgan
Thomas P Liddy
Joseph Eugene La Rue
Joseph Branco
Karen J Hartman-Tellez
Jack O'Connor
Sean M Moore
Rosa Aguilar
Emily M Craiger
Hon Peter A Thompson
Amy M Wood
David T Hardy
Ryan L Heath
Alexander Haberbush
Raymond L Billotte
Hon Joseph C Welty
Hon Jeff Fine,
Hon Danielle J Viola

RETRIEVED FROM DEMOCRACYDOCKET.COM

EXHIBIT 7

Redacted

RETRIEVED FROM DEMOCRACYDOCKET.COM

WILENCHIK & BARTNESS

— A PROFESSIONAL CORPORATION —



Dennis I. Wilenchik
diw@wb-law.com

WILENCHIK & BARTNESS
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
The Wilenchik & Bartness Building
2810 North Third Street Phoenix Arizona 85004

Licensed in
Arizona, Texas
and New York

Telephone: 602-606-2810 Facsimile: 602-606-2811

October 9, 2024

Via Email and Regular Mail

Joseph E. La Rue, Esq.
Thomas P. Liddy, Esq.
Deputy County Attorneys
Maricopa County Attorney's Office
225 West Madison Street
Phoenix, AZ 85003
LarueJ@mcao.maricopa.gov
LiddyT@mcao.maricopa.gov

**Re: Maricopa County's response to MCRC's Pre-Litigation
Demand Letter Regarding Maricopa County's Non-Compliance
With Arizona Election Law**

Dear Joe and Tom:

Thank you for your response letter dated October 3, 2024. It was substantively responsive to most but not all points raised in our pre-litigation demand letters dated September 19, 2024, and September 28, 2024, but there are still material factual assertions that we disagree with as discussed below which must be addressed. Absent that, MCRC remains concerned that Maricopa County ("Maricopa") will repeat its violations of Arizona law in the upcoming 2024 election. It is still my hope that we can resolve these issues in good faith with your cooperation.

Encryption Keys Employed in Maricopa's Election Systems

Maricopa does not dispute that Arizona law expressly requires that all voting system passwords "*not be a vendor-supplied password and must only be known by authorized users.*" [2023 Election Procedure Manual ("EPM") at p. 102; *see also* 2019 EPM at 96 (same requirement)]. You also agreed that the encryption keys are stored in plain text and not protected in a cryptographic module. However, you stated that "there was no encryption requirement in the VVSG 1.0, there was also no requirement regarding how encryption keys should be stored.... The VVSG 1.0 (2005) is silent on the subject." That is incorrect in two ways.

First, contrary to your statement, the VVSG specifically includes the requirements for data encryption (which Maricopa's Dominion systems employ), and also adopts the Federal Information Processing Standards ("FIPS") defining the mandatory practices for



WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —

Joe E. La Rue, Esq.
Thomas P. Liddy, Esq.
October 9, 2024
Page 2 of 7

management of cryptographic keys. [See, e.g., VVSG 1.0 (2005) § 7.5.1(b)(i), p. 125, Maintaining Data Integrity; § 7.7.3, p. 132, Protecting Transmitted Data; and § 7.9.3, p. 138, Electronic and Paper Record Structure subsection a].

Second, the EAC Scope of Conformance for DVS Democracy Suite 5.5B expressly states this voting system has been evaluated “for conformance” to VVSG 1.0, and the attached Scope of Certification for DVS Democracy Suite 5.5B expressly states that this election software employs a “FIPS 140-2 validated cryptographic module.”¹ Assuming that the Scope of Certification is accurate, the fact that the keys are readily accessible (unprotected and in plain text) means that the election software Maricopa is using must be different than the DVS Democracy Suite 5.5B election software approved by the EAC and the Arizona Secretary of State with the FIPS 140-2 validated cryptographic module implemented. If that is the case, it is a violation of A.R.S. § 16-442.

There is also no purported upgrade for encryption in DVS Democracy Suite 5.17 that would satisfy the FIPS 140-2 requirements because *anyone* with access to the SQL database has access to the encryption keys—giving them the capability to decrypt passwords other than their own or alter the configuration of election system components to manipulate election results. Your repeated assertions that storing the encryption keys in “plain text” does not violate EAC-certification requirements entirely misses the point—it is the fact that the keys are *unprotected* by encryption (such as a FIPS 140-2 cryptographic module as the EAC certification requires) which is itself a violation of EAC-certification requirements.

The next issue is the statement in your response letter that:

Encryption keys are not passwords. They are different than passwords and have a different function. They are machine generated, which is an industry best practice, and are not something that the County can generate or control. A password, on the other hand, is an authentication that is often adjusted based off of a user account and can be set by the owner of the system. The County can, and does, control these.

As I’m sure you know, the encryption keys used in Maricopa’s election system are not all the same and each key serves different purposes.² Because of this, there are several

¹https://www.eac.gov/sites/default/files/voting_system/files/DVS_5.5B_Certificate_Scope_Conformance.pdf at p. 12.

² As noted in our prior correspondence, the encryption keys are the Rijndael Key, the Rijndael Vector, the X509 certificate, and the Hash-Based Message Authentication Code (“HMAC”).



WILENCHIK & BARTNESS
A PROFESSIONAL CORPORATION

Joe E. La Rue, Esq.
Thomas P. Liddy, Esq.
October 9, 2024
Page 3 of 7

problems with your foregoing statements. First, as noted previously, given the lack of required protection for these encryption keys, any party with access to the SQL database also has access to these keys. That means the Rijndael Key and Vector can be obtained by unauthorized parties and used to *decrypt* e.g., tabulator passwords. This lack of protection for the Rijndael Key and Vector gives rise to a violation of Arizona law requiring that passwords “*must only be known by authorized users*” and is a major security vulnerability.

[REDACTED]

If a malicious individual gained knowledge of the Rijndael Key and Vector specific to an election, they could for example:

- Modify the programming of a tabulator, enabling them to alter the election results. This unauthorized access and manipulation would allow the malicious actor to alter votes and vote tallies or even create fake ballots without likely detection.
- Edit the results recorded by the tabulator before they are imported into the Election Management System and change the election results, again without likely detection

Second, contrary to your statement that the encryption keys are “machine generated ... and are not something that the County can generate or control,” the X509 certificate used by Maricopa in the 2020 [REDACTED]

[REDACTED] That certificate is code that includes public and private keys used to ensure the ballot images and election data are transmitted securely between authorized machines on Maricopa’s network that authenticate each other as the intended sender and recipient. Thus, the X509 certificate “is an authentication” code as you yourself define the function of a “password”³ and is employed in Maricopa on voting systems to be used in the 2024 election; yet it does not appear to be a unique, machine-generated code. Rather, it appears to be controlled and known by the vendor, Dominion, [REDACTED]

[REDACTED]

³ Password is similarly defined as “something that enables one to pass or gain admission: such as ... a sequence of characters required for access to a computer system or digital device.” <https://www.merriam-webster.com/dictionary/password>.



WILENCHIK & BARTNESS
A PROFESSIONAL CORPORATION

Joe E. La Rue, Esq.
Thomas P. Liddy, Esq.
October 9, 2024
Page 4 of 7

[REDACTED] is a serious security vulnerability and violates the EPM's prohibition of vendor-supplied passwords and mandate that passwords only be known by authorized users.

Vendor Supplied Passwords Employed in Maricopa's Election Systems

As noted in our previous correspondence, Dominion apparently inserted multiple common usernames and passwords into DVS systems [REDACTED]. These passwords and username combinations were present in DVS computing devices [REDACTED]. Two of these vendor supplied passwords (redacted here) [REDACTED]. There may be others. [REDACTED]. Any vendor-supplied password on an election system violates Arizona law.

Your claim that Maricopa doesn't use that vendor-supplied password is irrelevant. In fact, your statement these vendor-supplied passwords "are Dominion administrative passwords that Dominion uses to update core functionality of the EMS applications and services, such as Microsoft has Microsoft-specific authenticators built into their operating systems" is alarming because, contrary to your belief, in the wrong hands those core functions *can be used to manipulate election results* along with other pernicious activities. The existence of these vendor-supplied passwords on Maricopa's election software violates the EPM and is a major security vulnerability as the EPM implicitly recognizes. For example, these vendor-supplied passwords are apparently used to control the Election Event Designer and can be exploited to allow a user—including an insider threat—to create, change, or modify user accounts (e.g., "RTR Admin"), components (e.g., iButton credentials controlling tabulator functions), and applications on the DVS Democracy Suite election software, and thereby alter or manipulate election results.

Notably, Maricopa employs outside actors, including Dominion employees, to conduct elections—a classic insider threat vector which was recently brought to Maricopa's attention.⁵ Indeed, during the Arizona Senate audit, Maricopa revealed that it did not possess the administrative credentials for Maricopa's ICP2 tabulators. Instead, Dominion had sole possession of these credentials which could be used to control the

⁴ [REDACTED]

⁵ <https://www.fox10phoenix.com/news/more-details-revealed-about-theft-incident-maricopa-county-elections-building>



WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —

Joe E. La Rue, Esq.
Thomas P. Liddy, Esq.
October 9, 2024
Page 5 of 7

configuration settings of the tabulators, which in turn could allow vote manipulation. Your reliance on purported physical security of MTEC is not applicable to insider threats, offers no impediment to numerous threats targeting Maricopa’s network and election equipment, and is not an exception to Arizona law governing passwords.

Modifications to Democracy Suite 5.5B

With respect to MBS and Democracy Suite 5.5B you state:

[T]he County used the Dominion Democracy Suite 5.5B software in the 2020 and 2022 elections. This software, including its minor version 5.10.X.X, was certified and approved by the EAC for use in elections in the United States, and then certified and approved by the Arizona Secretary of State for use in Arizona, in 2019.

First, the terms “major” and “minor” do not appear in the published EAC certification, nor are these terms used in any report by the VSTLs. Second, contrary to your statements, this MBS configuration file was *not* tested as part of DVS D-Suite 5.5-B by a laboratory accredited per A.R.S. § 16-442(B), *not* certified by the EAC as part of DVS D-Suite 5.5-B, and *not* recommended to the Arizona Secretary of State for adoption by the Equipment Certification Advisory Committee. Dominion’s vendor documentation makes clear that the accuracy and reliability of the tabulators may be adversely affected by use of incorrect tabulator configuration files or settings. Third, the assertion that the double colon “::” in the MBS version 5.5-B::10 is a wildcard is simply incorrect. The “::” is not a standard wildcard in version control. It is a separator, not a range indicator. While the explanation about wildcards may apply elsewhere, it has no relevance here. As stated in the Scope of Conformance, the DVS D-Suite 5.5-B software version is expressly confined to the evaluated configuration and is not part of any flexible range as suggested.

Finally, Maricopa represented on its website that “[p]rior to the L&A [testing] ... a copy of the software is forwarded to the [SoS]” and “[p]rior to each election, the software and hash code are verified to confirm the software system being used for the election is the same system that underwent certification.” However, our experts reviewed the Maricopa DVS Democracy Suite 5.5B software purportedly used in the 2020 election and found that the software hash codes do *not* match the EAC-certified version. [See Cotton Decl. ¶¶21-22, 28-29].

L&A Testing

With respect to MCRC’s concerns that Maricopa may have a practice of loading memory cards with election software onto tabulators *after* the statutorily announced L&A



WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —

Joe E. La Rue, Esq.
Thomas P. Liddy, Esq.
October 9, 2024
Page 6 of 7

test date, you characterized this as being due to a programming mistake discovered just prior to the October 11, 2022 L&A test and that Maricopa was unaware of anything like that occurring after the October 6, 2020 L&A test. If that is true, then it should be easy for Maricopa to confirm that it will not load memory cards with election software onto tabulators *after* the statutorily announced L&A test date of October 8, 2024.

Conclusion

In light of the aforementioned, we ask that Maricopa confirm the following in writing by the close of business Monday, October 14, 2024:

1. Maricopa will protect the encryption keys on its election systems in accordance with EAC certification requirements and FIPS 140-2 as stated in the Scope of Certification.
2. Maricopa will ensure that Maricopa's current passwords cannot be decrypted by a user who is not authorized to know that specific password employing the Rijndael Key and Vector.
3. Maricopa will remove all vendor supplied passwords, including the Dominion licensed X509 certificate, from its election systems as mandated by the EPM. These items must be replaced with appropriate Maricopa specific credentials if they are to remain on the voting system.
4. Each of the passwords for each user account on a Windows based system is unique to that username and not shared with other usernames.
5. Each of the usernames on a Windows based system are assigned to a single individual (not shared) and that a log of assignment and access to these usernames is maintained as part of the election records.
6. There are no executable files (.exe, .dll, .bat, etc) on any of the systems that were created after the date of the installation of DVS 5.17.
7. After the completion of the official statutorily announced and compliant L&A test scheduled to take place on or about October 7, 2024, Maricopa will *not* reformat or alter the L&A-tested software configuration on any memory cards of any tabulator, or install any election software on any tabulator, without conducting a statutorily compliant L&A test on those tabulators in accordance with A.R.S. § 16-449 after taking such actions.



WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —

Joe E. La Rue, Esq.
Thomas P. Liddy, Esq.
October 9, 2024
Page 7 of 7

These are simple requests to comply with Arizona law. I do not know what else to do to assure our client of the integrity of the process and hope you will see it that way and be cooperative. If not, please tell me why you cannot do so and maybe we can discuss before I have to take action. My best personal regards to you and your colleagues there.

Sincerely Yours,

A handwritten signature in black ink, appearing to read 'Dennis I. Wilenchik', written in a cursive style.

Dennis I. Wilenchik

Enclosure

RETRIEVED FROM DEMOCRACYDOCKEY.COM

EXHIBIT 8

RETRIEVED FROM DEMOCRACYDOCKET.COM

WILENCHIK & BARTNESS
— A PROFESSIONAL CORPORATION —





Maricopa County Attorney
RACHEL MITCHELL

October 14, 2024

VIA EMAIL ONLY

Dennis Wilenchik, Esq.
Wilenchik & Bartness
2810 N. Third Street
Phoenix, AZ 85004

RE: Your October 9, 2024, letter on behalf of the MCRC

Dear Dennis:

Thank you for your October 9, 2024, letter, responding to our October 3 letter. We appreciate that you took the time to read our letter. We realize it was lengthy, but we wanted to provide you with the relevant facts to allow you to conduct the reasonable inquiry required by Rule 11.

Unfortunately, it appears that you continue to rely on the representations of Messrs. Olsen and Cotton, and perhaps Mr. Parikh, in your October 9 letter. We reviewed it with intellectual technology professionals who inform us that it contains a mixture of incorrect statements and nonsensical assertions. Further, it appears that your issues are with certification procedures adopted by the Election Assistance Commission and not with anything that is actually within the County's ambit.

You ask that the County comply with Arizona law in the upcoming election. It will, just as it did in 2022, and 2020, and elections before those.

Sincerely,

Thomas P. Liddy
Civil Division Chief

Joseph E. La Rue
Election Law Team Leader

EXHIBIT 9

Redacted

RETRIEVED FROM DEMOCRACYDOCKET.COM

WILENCHIK & BARTNESS

— A PROFESSIONAL CORPORATION —

Declaration of Clay U. Parikh

I, CLAY U. PARIKH, declare under penalty of perjury that the following is true and correct:

1. I have personal knowledge of the matters set forth below and would testify competently to them if called upon to do so.

2. I have a Master of Science in Cyber Security, Computer Science from the University of Alabama in Huntsville. I have a Bachelor of Science in Computer Science, Systems Major from the University of North Carolina at Wilmington. In February 2007 I obtained the Certified Information Systems Security Professional (CISSP) certification and continually maintained good standing, until I released it on 28 February 2024. I also held the following certifications: Certified Ethical Hacker (CEH) and Certified Hacking Forensic Investigator (CHFI).

3. Since December of 2003, I have continually worked in the areas of Information Assurance (IA), Information Security and Cyber Security. I have performed and led teams in Vulnerability Management, Security Test and Evaluation (ST&E) and system accreditation. I have supported both civil and Department of Defense agencies within the U.S. government as well as international customers, such as NATO. I have served as the Information Security Manager for enterprise operations at Marshall Space Flight Center, where I ensured all NASA programs and projects aboard the center met NASA enterprise security standards. I was also responsible in part for ensuring the Marshall Space Flight Center maintained its Authority to Operate (ATO) within the NASA agency. I have also served as the Deputy Cyber Manager for the Army Corps of Engineers where I led and managed several teams directly in: Vulnerability Management, Assessment and Authorization (A&A), Vulnerability Scanning, Host Based Security System (HBSS), Ports Protocols and Service Management, and an Information System Security Manager (ISSM) team for cloud projects. I also have performed numerous internal digital forensic audits. During this time span, I also worked at the Army Threat Systems Management Office (TSMO) as a member of the Threat Computer Network Operations Team (TCNOT). I provided key Computer Network Operations (CNO) support by performing

validated threat CNO penetration testing and systems security analysis. TCNOT is the highest level of implementation of the CNO Team concept.

4. From 2008 to 2017, I also worked through a professional staffing company for several testing laboratories that tested electronic voting machines. These laboratories included Wyle Laboratories, which later turned into National Technical Systems (NTS) and Pro V&V. My duties were to perform security tests on vendor voting systems for the certification of those systems by either the Election Assistance Commission (EAC), or to a state's specific Secretary of State's requirements.

5. I have analyzed the tabulator system log files produced by Maricopa in connection with the 2022 General Election. I also analyzed the system log files for Maricopa County's vote center tabulators used in the 2020 General Election as well the Maricopa County's election systems database and the forensic images of the vote center tabulator memory cards used in the 2020 General Election. I have also analyzed Dominion election databases in four Georgia counties, Mesa Colorado along with their system logs.

6. I have also reviewed the February 23, 2021, Audit Reports by Pro V&V¹ and SLI Compliance², the Maricopa County Forensic Election Audit Report conducted by Cyber Ninjas at the request of the Arizona Senate and related follow-on reports by Maricopa and responses thereto, and other documents relevant to my analysis as noted herein.

7. I make the following observations and conclusions based on this information.

EXECUTIVE SUMMARY

8. Given my education, experience as a security professional and years of experience working with Voting System Testing Laboratories (VSTL), and the thorough analysis of the systems, processes, and the electronic records detailed above, the facts have led to the conclusion that the voters of Maricopa County should have no confidence that their votes have been accurately counted, if they were even counted at all. The **egregious** security violation discovered,

¹ <https://www.maricopa.gov/DocumentCenter/View/66844/Post-Audit-Report>

² Case 2:22-cv-00677-JJT Document 29-8 Filed 06/07/22 "Exhibit 7"

concerning the encryption keys utilized by the voting system only reinforces this conclusion.

9. I understand Arizona law expressly requires that: “[components of the electronic voting system....[m]ust be password-protected (for voting system software).... [and that] passwords must not be a vendor-supplied password and must only be known by authorized users.” 2023 Election Procedure Manual (“EPM”) at p. 102; *See also* 2019 EPM at 96.³ As detailed below, Maricopa County is violating these requirements in multiple ways

10. Maricopa County uses a vote center model to conduct elections. This model includes a central facility (MCTEC) where the Election Management System (EMS) and high-speed tabulator/scanners are located. There are also more than two hundred vote centers (i.e., polling locations) throughout the county each with two ImageCast Precinct-2 (ICP2) tabulators to scan and process ballots. Tabulator memory cards contain the election software programming for each election and are inserted into every tabulator/scanner allowing them to read and tabulate the ballots for that election.

11. Analysis of the 2020 election database revealed the most egregious security violation. The secret cryptographic encryption keys and x509 certificate used to encrypt, decrypt, the election data, and used for authentication when transferring files and communication are stored in plaintext, unprotected within the election database. With these items anyone could manipulate system configuration files causing the tabulators to not function properly. They could create or duplicate election data and make it look authentic. The possible attacks or manipulation of data are endless.

12. In addition, it appears that Dominion inserted multiple common usernames and passwords [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] | [REDACTED] With these vendor

³ https://apps.azsos.gov/election/files/epm/2023/EPM_20231231_Final_Edits_to_Cal_1_11_2024.pdf and [https://azsos.gov/sites/default/files/docs/2019 Election Procedures Manual.pdf](https://azsos.gov/sites/default/files/docs/2019_Election_Procedures_Manual.pdf)

[REDACTED]

supplied passwords, Dominion or any other actor with licit or illicit access to Maricopa County’s voting system can, manipulate the voting system, election data, etc.

13. Compounding these security vulnerabilities is the fact that the database is not configured to standard security configurations used for a database dealing with sensitive information.

14. To further compound this egregious violation, proper account and password management are not being followed. Many user accounts and login passwords were found to be identical, making auditing or system troubleshooting almost impossible. This also can allow for an unauthorized user to access to an account.

15. Lastly, the x509 certificate found on and used by the Maricopa voting system [REDACTED] [REDACTED] The purpose of the security certificate serves the same function of authentication like a password in that it allows a system or a system component to authenticate to and/or trust another system or system component. [REDACTED] [REDACTED] exponentially increases the likelihood that an unauthorized user can gain access to Maricopa County’s election system.

DETAILED FINDINGS AND CONCLUSIONS

16. A.R.S. § 16-442(B) states that an electronic voting machines “may only be certified for use in this state and may only be used in this state if they comply with the Help America Vote Act (HAVA) of 2002 and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to the help America vote act of 2002.”

17. Maricopa acknowledges these requirements on its website⁵, stating further that: “The Dominion Democracy Suite 5.5B is both federally and state certified.” “The U.S. Election Assistance Commission certification is an official recognition that a voting system has been tested and has met an identified set of Federal voting system standards.”

⁵ <https://www.maricopa.gov/5539/Voting-Equipment-Facts>

18. Electronic voting systems overall are full of vulnerabilities with multiple exploits available. The vulnerabilities range from outdated Operating Systems (OS), third party applications, to protocols and services. Adding to these weaknesses is system configuration. Nearly all aspects of the voting systems do not use standard security, let alone industry best practices when configuring their systems. Voting system vendors, like Dominion, lack basic configuration management of their systems.

19. The election database is a prime example of misconfiguration. It is standard practice for a database to not use OS authentication to access or modify the database. Democracy Suite versions use OS authentication, which increases the number of attack vectors on the database. Additionally, if a database is to hold sensitive data it should be configured to encrypt the table, column, or row to which the sensitive data is to reside. This prevents anyone with read only or unauthorized access from seeing the data.

20. Lastly, Democracy Suite systems use a combination of a Rijndael Key, a Rijndael Vector, a Hash-based Message Authentication Code (HMAC) and a x509 security certificate to encrypt, decrypt and to authenticate data. These cryptographic keys are considered highly secret and should be kept hidden and protected. All of the components listed above (security processes) should be stored encrypted, especially if stored within a database. In the Democracy Suite systems, they are not. They are left unprotected and out in the open easy to find. With these items anyone could manipulate system configuration files causing the tabulators to not function properly. They could create or duplicate election data and make it look authentic. The possibilities are endless.

21. Furthermore, the plaintext storage of passwords and cryptographic keys on **any** information system, let alone a voting system, is an **egregious, inexcusable** violation of long-standing, **basic** cybersecurity best practices. It destroys any type of security the system wishes to implement. Windows log-in is the only authentication needed to access the unprotected database where the keys are stored. Windows log-in can easily be bypassed.⁶

22. These keys being plaintext outside of the cryptographic module also **violates** FIPS

⁶ https://www.youtube.com/watch?v=2v-mGf4_9-A

140-2. Section 4.7 of FIPS 140-2 “Cryptographic Key Management”⁷ states "The security requirements for cryptographic key management encompass the entire lifecycle of cryptographic keys[.]" The section also states that "Secret keys, private keys, and CSPs shall be protected within the cryptographic module from unauthorized disclosure, modification, and substitution." Section 4.7.5 “Key Storage” states "Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorized operators." Additionally, the National Institute of Standards and Technology NIST SP 800-57⁸ section 4.7 “Key Information Storage” states "The integrity of all key information **shall** be protected; the confidentiality of secret and private keys and secret metadata **shall** be protected. When stored outside a cryptographic module[.]"

23. In technology, it is best practice to assign unique user names to accounts and ensure user passwords are specific to the authorized user. Secrecy of an account password is paramount to security. This practice is even mandated in both the 2019 and 2023 Arizona EPM. However, generic account names and common passwords are found throughout the election database. See figures A-1 and A-2 in **Exhibit A**.

24. Of note regarding the technical and supervisor passcodes, the string of numbers repetitively used as a passcode in the Maricopa voting systems [REDACTED] [REDACTED] [REDACTED] increases the risk of possible exploitation exponentially. [REDACTED]

25. Another anomaly like the one mentioned above also exists with some of the administrative account passwords and security codes. [REDACTED] [REDACTED] [REDACTED] This is highly suspicious but more importantly it is a security concern.

26. Worse than the use of common passwords between different accounts, is the storage

⁷ <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf> pg.30

⁸ <https://doi.org/10.6028/NIST.SP.800-57pt2r1>

of these passwords themselves. Passwords are stored in both hash form and encrypted within the election database. The problem with this method is they are unprotected. Practically anyone can gain access to the database and copy the hash or encrypted password can discover the plain text password and utilize it. For example, one common hash for several admin accounts can easily be cracked using a public web site hashes.com. See figure B-1 in **Exhibit B**. The password [REDACTED] is a vendor supplied password, which violates both the Arizona 2019 and 2023 EPM. [REDACTED]

27. Another issue with this storage method, is that the secret encryption keys used to encrypt the passwords are also stored in this same vulnerable database. The keys are stored in plaintext. See figure B-2 in **Exhibit B**. Using the Rijndael key and vector, the encrypted passwords can easily be decrypted on a public website. For example, see figure B-3 in **Exhibit B** where a tabulator admin password is decrypted. Again, note that all the tabulator admin accounts have the same password. With that single password you could access any tabulator.

28. The EAC Certification *Scope of Conformance* defines the specific software and firmware component versions tested and certified by both the EAC and the state of Arizona. An extract of page 12 from the EAC's DVS 5.5B certification⁹ is attached as **Exhibit C**. The EAC Certificate of Conformance for Democracy Suite 5.5B states that the FIPS 140-2 cryptographic module is implemented as part of the voting system.

29. It is understood that Maricopa County does not use DVS 5.5B any longer and is now at DVS version 5.17. Note that the upgrade to DVS 5.17 will not prevent half the attacks on the system that could occur due to the vulnerabilities and violations listed in this document. The response back from the Maricopa's attorneys about having to "de-encrypt" the EMS hard drive is equally ineffective.¹⁰ Drive encryption does not address the multiple remote and local vulnerabilities on the system. Nor does it take into account insider threat. Additionally, hard drive encryption also does not meet FIPS 140-2 requirement least access for containers. This

⁹ https://www.eac.gov/sites/default/files/voting_system/files/DVS_5.5B_Certificate_Scope_Conformance.pdf

¹⁰ Letter to Dennis Wilenchik dated October 3, 2024 at page 6.

only stops unauthorized users from gaining access to the volume when the system is down. Anyone gaining access to the system while it is up, either remotely or local will have access to the encryption keys.

CONCLUSION

30. The appalling account management, storage of passwords and encryption keys, and use of vendor supplied passwords violates the EPM's password requirements which I understand has the force of law. [REDACTED]

[REDACTED] The encryption mechanisms and security certificates are left totally unprotected in a highly vulnerable system. The result of these critical faults, individually or collectively, if allowed to remain on Maricopa County's election system, means there would be no way to know if votes cast in the 2024 election were correctly recorded or tabulated.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 21 day of October 2024.


s/ 
Clay U. Parikh

Exhibit A



Figure A-1. Common password hashes



Figure A-2. Common accounts and passwords (encrypted)

Exhibit A



Figure A-3. Common password across states and counties



Figure A-4. [REDACTED]

Exhibit B



Figure B-1. hashes.com Dominion admin password



Figure B-2. Secret encryption key, vector and certificate

Exhibit B

anycrypt.com/crypto

Base64 HEX

Encrypt

AES Decryption

Encrypted Text

tdxJBrhv V31rldA==

Decrypted Text

11 311

Secret Key

c\$2J7Y% -A0

Encryption Key Size

128 Bits 192 Bits 256 Bits

Encryption Mode

CBC ECB

IV (optional)

7a\$K& Bp?3

Input format

Base64 HEX

View Format

Text JSON

Decrypt

RETRIEVED FROM DEMOCRACYDOCKET.COM

Figure B-3. Decrypted password with secret encryption key

Exhibit C

Feature/Characteristic	Yes/No	Comment
Local Area Network – Use of TCP/IP	YES	Client/server only
Local Area Network – Use of Infrared	NO	
Local Area Network – Use of Wireless	NO	
FIPS 140-2 validated cryptographic module	YES	
Used as (if applicable):		
Precinct counting device	YES	ImageCast Precinct
Central counting device	YES	ImageCast Central

Baseline Certification Engineering Change Orders (ECO)

ECO #	Component	Description
100503	ICP PCOS-320C & ICP PCOS-320A	Adding a COTS collapsible ballot box to AVL for use with the ICP
100521	Servers and Workstations	Added DELL P2419H monitor as a display device.
100527	EMS Workstations.	Added DELL Latitude 3490 computer with updated i3-8130U processor (Dual Core, 4MB Cache, 2.2GHz) to QVS PN 190-000061 (a client workstation).
100543	ICC Scanner	Update to the DR-G1130 Scanner LCD Panel User Interface.
100588	ICX Workstation	Added new models of VVPAT printer for use with the D-Suite ICX workstation due to previous model becoming commercially unavailable
100596	EMS Workstation	Added DELL Latitude 3400 computer as a client workstation due to the DELL Latitude 3490 computer becoming commercially unavailable for purchase
100597	EMS Server	Added DELL PowerEdge R640 computer with new processor and RAM as an AVL to the existing R640 server computer configurations
100602	EMS Server and Workstations	Added DELL Precision 3431 computer in an EMS Express Server and EMS Client Workstation configuration due to the DELL Precision 3430 computer becoming commercially unavailable for purchase
100603	ICC Scanner	Added DELL P2418HT monitor as a display device for ICC HiPro scanner workstation configuration due to the Lenovo 10QXPAR1US monitor becoming commercially unavailable for purchase